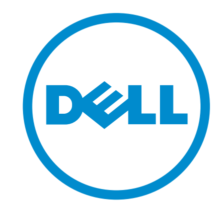
OpenManage Integration for VMware vCenter für Web-Client

Benutzerhandbuch Version 2.3



Anmerkungen, Vorsichtshinweise und Warnungen



ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.



VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.



WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2015

Rev. A00

Inhaltsverzeichnis

1

Einführung

VMware vCenter ist die primäre Konsole für IT-Administratoren zur Verwaltung und Überwachung von VMware vSphere-ESX/ESXi-Hosts. In einer standardisierten, virtualisierten Umgebung werden VMware-Warnungen und -Überwachung dazu verwendet, Sie aufzufordern, zur Behebung von Hardwareproblemen eine separate Konsole zu starten. OpenManage Integration for VMware vCenter ist ein Produkt, mit dem Sie die VMware vCenter-Server innerhalb des VMware Web-Clients verwalten können, sodass Sie nicht mehr an ein Windows-System gebunden sind. Mithilfe von OpenManage Integration for VMware vCenterhaben Sie Funktionen zur Verwaltung und Überwachung von Dell Hardware in der virtualisierten Umgebung, wie z. B.:

- Warnungen und Umgebungsüberwachung: Erkennen wichtiger Hardware-Fehler und Durchführen virtualisierungsbezogener Maßnahmen (zum Beispiel Migrieren von Arbeitslasten oder Versetzen von Hosts in den Wartungsmodus).
- Single-Server-Überwachung und -Berichterstellung: Überwachung und Berichtsfunktionen von Servern.
- Firmware-Aktualisierungen: Aktualisieren von Dell-Hardware auf die aktuellste Version des BIOS und der Firmware.
- Erweiterte Bereitstellungsoptionen: Erstellen von Hardware- sowie Hypervisor-Profilen und Bereitstellen einer beliebigen Kombination dieser beiden auf Dell PowerEdge-Bare-Metal-Servern, remote und ohne PXE – mithilfe von vCenter.

OpenManage Integration for VMware vCenter

Verwenden Sie OpenManage Integration for VMware vCenter zur Ausführung von:

Bestandsaufnahme	Bestandsaufnahme von wichtigen Ressourcen, Durchführen von Konfigurationsaufgaben sowie Bereitstellen von Cluster- und Datencenteransichten der Dell-Plattformen.
Überwachung und Warnmeldungen	Entdecken von Schlüssel-Hardware-Fehlern und Durchführen von virtualisierungsorientierten Aktionen (z. B. Migration von Arbeitslasten oder das Umstellen von Hosts in den Wartungsmodus) ausführen. Geben Sie zusätzliche Informationen (Bestandsaufnahme, Ereignisse und Alarme), um Server-Probleme zu diagnostizieren. Erstellen von Berichten im Rechenzentrum und in der Cluster-Anzeige und Export zu einer CSV-Datei.
Firmware-Aktualisierungen	Aktualisieren von Dell-Hardware auf die aktuellste Version des BIOS und der Firmware.
Bereitstellung	Erstellen von Hardwareprofilen Hypervisor-Profile und Remote-Bereitstellung einer beliebigen Kombination der beiden On-Bare-Metal-PowerEdge-Servern von Dell unter Verwendung von VMware vCenter, ohne Einsatz von PXE.
Service-Informationen	Abrufen von Dell-Garantieinformationen aus dem Internet.
Sicherheitsrollen und Berechtigungen	Integration mit Standardauthentifizierung, -rollen und -berechtigungen von vCenter.

2

Wie OpenManage Integration for VMware vCenter konfiguriert oder bearbeitet werden kann

Nachdem Sie die grundlegende Installation von OpenManage Integration for VMware vCenter beenden, wird der Erstkonfigurationsassistent angezeigt, wenn Sie das Dell OpenManage Integration-Symbol anklicken. Verwenden Sie den Erstkonfigurationsassistenten, um die Einstellungen beim ersten Start zu konfigurieren. Für nachfolgende Instanzen verwenden Sie die Seite **Einstellungen**. Vom Erstkonfigurationsassistenten aus können Sie außerdem die Einstellungen der Garantie, Bestandsaufnahme, Ereignisse und Alarme bearbeiten. Obwohl der Einsatz des Erstkonfigurationsassistenten die am häufigsten verwendete Methode ist, können Sie diese Aufgabe auch über die Seite **OpenManage Integration** → **Verwalten** → **Einstellungen** des Geräts in der OpenManage Integration for VMware vCenter ausführen. Weitere Informationen zum Erstkonfigurationsassistenten finden Sie im **Benutzerhandbuch zur OpenManage Integration für VMware vCenter**.

Konfigurationstasks im Konfigurationsassistenten

Der Erstkonfigurationsassistent kann zur Konfiguration der folgenden Einstellungen für ein vCenter oder für alle registrierten vCenters verwendet werden:

1. vCenter-Auswahl
2. Erstellen eines neuen Verbindungsprofils
3. Planen von Bestandsaufnahme-Jobs
4. Ausführen eines Garantieabfrage-Jobs
5. Konfigurieren von Ereignissen und Alarmen



ANMERKUNG: Sie können den Erstkonfigurationsassistenten auch unter Verwendung des Links **Erstkonfigurationsassistent starten** unter **Grundlegende Tasks** auf der Seite **Erste Schritte** starten.

Willkommens-Seite im Konfigurationsassistent

Nach der Installation der OpenManage Integration for VMware vCenter muss sie konfiguriert werden.

1. Klicken Sie im **vSphere Web-Client** auf die **Startseite** und dann auf das Symbol **OpenManage Integration**
2. Beim ersten Klicken auf das Symbol **OpenManage Integration** wird der **Konfigurationsassistent** geöffnet. Sie können auch auf der Seite **OpenManage Integration** → **Erste Schritte** → **Erstkonfigurationsassistent starten** auf diesen Assistenten zugreifen.

vCenter-Auswahl

Die vCenter-Auswahlseite ermöglicht Ihnen die Auswahl eines spezifischen vCenter, um es zu konfigurieren oder die Auswahl aller vCenter, um sie zu konfigurieren.

1. Klicken Sie im **Erstkonfigurationsassistent** auf **Weiter** auf dem **Willkommens**bildschirm.
2. Wählen Sie ein oder alle vCenter aus der **vCenters**-Dropdown-Liste. Wählen Sie ein einzelnes vCenter für die noch nicht konfigurierten oder falls Sie Ihrer Umgebung ein neues vCenter hinzugefügt haben. Die vCenter-Auswahlseite ermöglicht Ihnen die Auswahl eines oder mehrerer vCenter zur Konfiguration ihrer Einstellungen.
3. Klicken Sie auf **Weiter,** um zur Beschreibungsseite des Verbindungsprofils zu gelangen.

Erstellen eines neuen Verbindungsprofils mit Hilfe des Erstkonfigurationsassistenten

Ein Verbindungsprofil speichert den iDRAC und die Host-Anmeldeinformationen, die das virtuelle Gerät für die Kommunikation mit Dell Servern verwendet. Jeder Dell Server muss einem Verbindungsprofil zugeordnet sein, damit er vom Dell OpenManage Integration for VMware vCenter verwaltet werden kann. Sie können mehrere Server einem einzelnen Verbindungsprofil zuweisen. Das Verfahren zum Erstellen des Verbindungsprofils ist im Konfigurationsassistenten und in der Option **OpenManage Integration for VMware vCenter** → **Einstellungen** nahezu identisch.

Sie können sich unter Verwendung der Active Directory-Anmeldeinformationen am iDRAC und Host anmelden. Vor der Verwendung der Active Directory-Anmeldeinformationen mit einem Verbindungsprofil muss das Active Directory-Benutzerkonto in Active Directory vorhanden sein, und iDRAC und Host müssen für die Active Directory-basierte Authentifizierung konfiguriert sein.



ANMERKUNG: Die Active Directory-Anmeldeinformationen können für iDRAC und Host identisch sein oder sie können als separate Active Directory-Anmeldeinformationen festgelegt werden. Die Benutzeranmeldeinformationen müssen Administratorrechte aufweisen.



ANMERKUNG: Sie können ein Verbindungsprofil nicht erstellen, falls die Anzahl an hinzugefügten Hosts das Lizenzlimit zur Erstellung eines Verbindungsprofils überschreitet.

So erstellen Sie ein neues Verbindungsprofil mithilfe des Assistenten:

1. Klicken Sie von der Seite **Verbindungsprofilbeschreibung** aus auf **Weiter**, um fortzufahren.
2. Geben Sie auf der Seite **Name und Anmeldeinformationen** den **Verbindungsprofilnamen** und eine optionale **Verbindungsprofilbeschreibung ein.**
3. Führen Sie auf der Seite **Name und Anmeldeinformationen** unter **iDRAC-Anmeldeinformationen** eine der folgenden Optionen aus:

   ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.

   - Für iDRACs, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.

     – Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domäne/Benutzername oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.

  - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
  - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
  - Führen Sie eine der folgenden Aktionen aus:
    - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
    - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
- Um iDRAC-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:
  - Geben Sie im Textfeld **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Weitere Informationen zur Benutzername-Einschränkungen für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.
  - Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
  - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
  - Führen Sie eine der folgenden Aktionen aus:
    - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
    - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

4. Führen Sie im Host-Root-Bereich eine der folgenden Aktionen aus:
   - Für Hosts, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um Ihre Host-Anmeldeinformationen zu konfigurieren.
     - Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domäne/Benutzername oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten.

       Host-Benutzernamen und Domäne-Einschränkungen finden Sie in den folgenden Informationen:

       Host-Benutzername-Anforderungen:

       a. Zwischen 1 und 64 Zeichen lang
       b. Keine nicht-druckbaren Zeichen
       c. Ungültige Zeichen: " / \ [ ] : ; | = , + * ? < > @

       Host-Domänen-Anforderungen:

       a. Zwischen 1 und 64 Zeichen lang
       b. Das erste Zeichen muss ein alphabetisches Zeichen sein.
       c. Es kann kein Leerzeichen enthalten.
       d. Ungültige Zeichen: " / \ : | , * ? < > ~ ! @ # $ % ^ & ' ( ) { } _
     - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

– Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.

– Führen Sie eine der folgenden Aktionen aus:

  * Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

  * Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

- Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:

  – Im Textfeld **Benutzername** ist der Benutzername root. Dies ist der Standardbenutzername und Sie können den Benutzernamen nicht ändern. Falls das Active Directory jedoch eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, mit Ausnahme von root.

  – Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

  ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für ESX- und ESXi-Hosts verwendet werden.

  – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.

  – Führen Sie eine der folgenden Aktionen aus:

    * Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

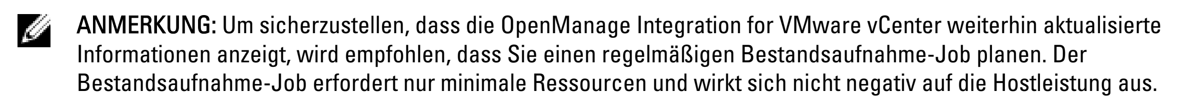
    * Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken Sie auf **Weiter**.
7. Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus und wählen die Schaltfläche **Verbindung testen**. Dieser Schritt ist optional. Dies wird zur Prüfung verwendet, ob der Host und die iDRAC-Anmeldeinformationen korrekt sind oder nicht.
8. Klicken Sie zum Vollenden des Profils auf **Weiter**. Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest „Für dieses System nicht anwendbar".

Planen von Jobs zum Erstellen von Bestandsaufnahmen [Assistent]

Die Konfiguration des Bestandsaufnahmezeitplans ist zwischen den Konfigurationsassistenten gleich. Gehen Sie zu

OpenManage-Integration– >**Verwalten**– >**Einstellungen**



ANMERKUNG: Um sicherzustellen, dass die OpenManage Integration for VMware vCenter weiterhin aktualisierte Informationen anzeigt, wird empfohlen, dass Sie einen regelmäßigen Bestandsaufnahme-Job planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

ANMERKUNG: Ein Gehäuse wird automatisch erkannt, sobald die Bestandsaufnahme für alle Hosts ausgeführt wird. Wenn das Gehäuse einem Gehäuse-Profil hinzugefügt wird, dann wird die Gehäusebestandsaufnahme automatisch ausgeführt. In einer SSO-Umgebung mit mehreren vCentern wird die Gehäusebestandsaufnahme bei jedem vCenter automatisch ausgeführt, wenn zu einem festgelegten Zeitpunkt die vCenter-Bestandsaufnahme für ein beliebiges vCenter ausgeführt wird.

So planen Sie einen Bestandsaufnahme-Job:

1. Aktivieren Sie im **Konfigurationsassistent** im Fenster **Bestandsaufnahme-Zeitplan** das Kontrollkästchen **Bestandsaufnahme-Datenabruf aktivieren**, sollte das Kontrollkästchen nicht aktiviert sein. Standardmäßig ist es aktiviert.

- Das Kontrollkästchen **Abrufen von Bestandsaufnahmedaten** wird standardmäßig markiert, um Ihnen das Planen der Bestandsaufnahme zu ermöglichen.

2. Führen Sie unter **Zeitplan für den Abruf von Bestandsaufnahmedaten** Folgendes aus:
   a. Markieren Sie das Kontrollkästchen neben jedem Wochentag, an dem Sie die Bestandsaufnahme ausführen möchten. Standardmäßig sind **alle Tage** markiert.
   b. Geben Sie die Uhrzeit in dem Format HH:MM in das Textfeld ein.

      Die Zeit, die Sie eingeben, ist Ihre lokale Zeit. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.
3. Um die Änderungen anzuwenden und fortzufahren, klicken Sie auf **Weiter**, um mit den Garantiezeitplaneinstellungen fortzufahren.

Ausführen eines Garantieabfrage-Jobs [Assistent]

Die Konfiguration des Garantieabfrage-Jobs kann in der Einstellungsoption in OpenManage Integration for VMware vCenter festgelegt werden. Darüber hinaus können Sie den Garantieabfrage-Job auch über die **Job-Warteschlange–>Garantie** ausführen. Geplante Jobs werden in der Job-Warteschlange aufgelistet. In einer SSO-Umgebung mit mehreren vCentern wird die Gehäuse-Garantie automatisch mit jedem vCenter ausgeführt, wenn die Garantie von einem beliebigen vCenter ausgeführt wird. Die Gewährleistung wird nicht automatisch ausgeführt, wenn es zu einem Gehäuse-Profil hinzugefügt wird.

So führen Sie einen Garantieabfrage-Job aus:

1. Im **Konfigurationsassistenten** im Fenster **Garantiezeitplan**

   - Markieren Sie das Kontrollkästchen **Garantiedatenabruf aktivieren**, um das Planen der Garantie zu ermöglichen.
2. Führen Sie unter **Garantiedatenabrufzeitplan** eine der folgenden Aktionen aus:
   a. Aktivieren Sie das Kontrollkästchen neben den Wochentagen, an denen die Garantie ausgeführt werden soll.
   b. Geben Sie die Uhrzeit in dem Format HH:MM in das Textfeld ein.

      Die Zeit, die Sie eingeben, ist Ihre lokale Zeit. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.
3. Um die Änderungen anzuwenden und fortzufahren, klicken Sie auf **Weiter**, um mit den **Alarm und Ereignis**-Einstellungen fortzufahren.

Konfigurieren von Ereignissen und Alarmen [Assistent]

Konfigurieren Sie Ereignisse und Alarme unter Verwendung des Konfigurationsassistenten oder von der Einstellungsoption für Ereignisse und Alarme von Dell OpenManage Integration für VMware vCenter aus.



ANMERKUNG: Verwenden Sie auf Hosts vor Dell PowerEdge-Servern der 12. Generation die Option „Host-Konformitätprobleme beheben“ zur Konfiguration der HostTrap-Liste in OMSA, um die Hostereignisse in vCenter anzuzeigen.

So konfigurieren Sie Ereignisse und Alarme:

1. Wählen Sie im **Erstkonfigurationsassistenten** unter **Anzeigeebenen für das Ereignis** eine der folgenden Optionen:

   - Keine Ereignisse übermitteln – Hardware-Ereignisse blockieren.
   - Alle Ereignisse übermitteln – Alle Hardware-Ereignisse übermitteln.
   - Nur kritische Ereignisse und Warnungsereignisse übermitteln – Nur kritische und Warnungsereignisse der Hardware übermitteln.

- Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung übermitteln – Nur kritische und Warnungsereignisse im Zusammenhang mit der Virtualisierung übermitteln. Dies ist die Standardeinstellung für die Übermittlung von Ereignissen.

2. Aktivieren Sie das Kontrollkästchen **Alarme für Dell-Hosts aktivieren**, um alle Hardware-Alarme und -ereignisse zu aktivieren.

   ANMERKUNG: Dell-Hosts, auf denen Alarme aktiviert sind, reagieren auf einige spezifische kritische Ereignisse, indem sie in den Wartungsmodus übergehen.

3. Ein Dialogfeld **Aktivieren der Dell-Alarmwarnung** wird angezeigt, klicken Sie auf **Weiter**, um die Änderung zu akzeptieren, oder klicken Sie auf **Abbrechen**.

   ANMERKUNG: Dieser Schritt wird nur dann angezeigt, wenn **Alarme für Dell Hosts aktivieren** ausgewählt wurde.

   ANMERKUNG: Nach dem Wiederherstellen des Geräts werden die Einstellungen für die Ereignisse und Alarme nicht aktiviert, selbst wenn sie die grafische Benutzeroberfläche als aktiviert anzeigt. Sie müssen die Einstellungen für die Ereignisse und Alarme auf der Seite „Einstellungen" erneut aktivieren

4. Um den Assistenten fortzusetzen, klicken Sie auf **Anwenden**.

3 Informationen zur VMware vCenter Web Client-Navigation

Die Navigation im VMware vCenter ist einfach. Wenn Sie sich am VMware vCenter anmelden und auf die Startseite und Start-Registerkarte gelangen, befindet sich das Dell Home-Symbol im Hauptinhaltsbereich unter der Gruppe „Administration“. Verwenden Sie das Dell Home-Symbol, um die Registerkarten und die Dell-Gruppe im Navigationsbereich (Navigator-Bereich) ausfindig zu machen.

Das VMware vCenter-Layout enthält die folgenden drei Abschnitte:

Navigator	Der Navigator-Bereich ist das primäre Menü, das für den Zugriff auf die verschiedenen Anzeigen auf der Konsole verwendet wird. OpenManage Integration for VMware vCenter hat eine spezielle Gruppe unter dem vCenter-Menü, das als primärer Zugriffspunkt für die OpenManage Integration for VMware vCenter dient.
Hauptinhaltsbereich	Zeigt die im Navigator ausgewählten Ansichten an. Der Hauptinhaltsbereich ist der Bereich, in dem die meisten Inhalte angezeigt werden.
Benachrichtigungen	Zeigt vCenter-Alarme und in Bearbeitung befindliche Tasks an. OpenManage Integration for VMware vCenter integriert sich in die Alarm-, Ereignis- und Tasksysteme in vCenter, um seine eigenen Informationen im Benachrichtigungsbereich anzuzeigen.

Navigation zur OpenManage Integration for VMware vCenter innerhalb des VMware vCenter

Die OpenManage Integration for VMware vCenter befindet sich in einer speziellen Dell-Gruppe innerhalb des VMware vCenters.

1. Melden Sie sich an VMware vCenter an.
2. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol OpenManage Integration.

   Von hier aus können Sie von den Registerkarten im Hauptinhaltsbereich aus die Verbindungsprofile der OpenManage Integration for VMware vCenterund die Produkteinstellungen verwalten, die Bestandsliste und Garantiejobs überwachen, die Zusammenfassungsseite anzeigen und vieles mehr.
3. Wählen Sie zum Überwachen von Hosts, Datacenters und Clusters im Navigator auf der linken Seite unter „Bestandslisten“ den Host, das Datacenter oder den Cluster aus, den Sie untersuchen wollen, und klicken Sie anschließend auf der Registerkarte „Objekt“ auf das gewünschte Objekt.

Verstehen der Symbolschaltflächen

Die Benutzerschnittstelle des Produkts verwendet viele symbolbasierte Aktionsschaltflächen für die ergriffenen Maßnahmen.

Tabelle 1. Symbolschaltflächen definiert

Symbolschaltfläche	Definition
	Verwenden Sie dieses Symbol mit dem Plus-Zeichen, um etwas hinzuzufügen oder etwas Neues zu erstellen.
	Verwenden Sie dieses Symbol zum Hinzufügen eines Servers, um einem Verbindungsprofil, Datenzenter und Cluster einen Server hinzuzufügen.
	Verwenden Sie dieses Symbol, um einen Job abzubrechen
	Verwenden Sie dieses Symbol, um eine Liste zu verkleinern.
	Verwenden Sie dieses Symbol, um eine Liste zu erweitern.
	Verwenden Sie dieses Symbol, um ein Objekt zu löschen.
	Verwenden Sie dieses Symbol, um einen Zeitplan zu ändern.
	Verwenden Sie dieses Bleistift-Symbol zur Bearbeitung.
	Verwenden Sie dieses Besensymbol, um einen Job zu löschen.
	Verwenden Sie dieses Symbol, um eine Datei zu exportieren.

Die Softwareversion suchen

Die Softwareversion befindet sich auf der Registerkarte für erste Schritte in OpenManage Integration for VMware vCenter.

1. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol OpenManage Integration.
2. Klicken Sie auf die **Versionsinformationen** auf der Registerkarte für erste Schritte in OpenManage Integration for VMware vCenter
3. Zeigen Sie die Versionsinformationen im Dialogfeld „Versionsinformationen“ an.
4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Aktualisieren des Bildschirminhalts

Sie können den Bildschirm jederzeit durch Verwendung des VMware vCenter„Aktualisieren“-Symbols aktualisieren.

1. Wählen Sie eine Seite aus, die Sie aktualisieren lassen wollen.
2. Klicken Sie in der VMware vCenter-Titelleiste auf die Schaltfläche **Aktualisieren**.

   Das „Aktualisieren“-Symbol befindet sich links neben dem Suchbereich („Suche“) und ähnelt einem dem Uhrzeigersinn folgenden Pfeil.

Anzeigen der Lizenzregisterkarte OpenManage Integration for VMware vCenter

Wenn Sie die Lizenz für OpenManage Integration for VMware vCenter installieren, wird die Anzahl unterstützter Hosts und vCenters auf dieser Registerkarte angezeigt. Sie können auch die Version von OpenManage Integration for VMware vCenter oben auf der Seite anzeigen. Diese Seite unter **Lizenzverwaltung** hat Links zu:

- Produktlizenzierungsportal (Digital Locker)
- iDRAC-Lizenzierungsportal
- Verwaltungskonsole
- Lizenz kaufen

Zeigen Sie in OpenManage Integration for VMware vCenter auf der Lizenzierungsregisterkarte folgendes an:

	Lizenzierung
Hostlizenzen	• Verfügbare Lizenzen Zeigt die Anzahl der verfügbaren Lizenzen an. • In Verwendung befindliche Lizenzen Zeigt die Anzahl der in Verwendung befindlichen Lizenzen an.
vCenter-Lizenzen	• Verfügbare Lizenzen Zeigt die Anzahl der verfügbaren Lizenzen an. • In Verwendung befindliche Lizenzen Zeigt die Anzahl der in Verwendung befindlichen Lizenzen an.

Öffnen der Online-Hilfe

Sie können die Online-Hilfe von der Registerkarte 'Hilfe und Support' her öffnen. Sie können das Dokument nach Informationen über ein Thema oder einen Vorgang durchsuchen. Die Online-Hilfe enthält den Großteil des Benutzerhandbuchs.

1. Führen Sie in OpenManage Integration for VMware vCenter einen der folgenden Schritte aus:
   - Klicken Sie in Hilfe und Support, unter **Produkthilfe,** auf **OpenManage Integration for VMware vCenter-Hilfe**.
2. Verwenden Sie die Inhaltsangabe im linken Bereich oder suchen Sie nach dem gewünschten Thema.
3. Wenn Sie mit der Hilfe fertig sind, klicken Sie in der oberen rechten Ecke auf das **rote X**.

Hilfe und Support finden

Um Ihnen die Informationen bereitzustellen, die Sie über Ihr Produkt brauchen, bietet OpenManage Integration for VMware vCenter das Register „Hilfe und Support“. In diesem Register können Sie die folgenden Informationen finden:

Produkthilfe	Stellt folgende Links bereit: • Hilfe für OpenManage Integration for VMware vCenter Stellt einen Link zur Produkthilfe bereit, die sich im Produkt befindet. Verwenden Sie das Inhaltsverzeichnis oder Suche, um die Hilfe, die Sie brauchen, zu finden. • Info Dieser Link ruft das Dialogfeld der Versionsinformationen auf. Sie können die Produktversion hier finden.
Dell Handbücher	Stellt Live-Links für Folgendes bereit: • Server-Handbücher

	• Hilfe für OpenManage Integration for VMware vCenter
Verwaltungskonsole	Stellt einen Link zur Verwaltungskonsole bereit
Zusätzliche Hilfe und Support	Stellt Live-Links für Folgendes bereit: • iDRAC mit Lifecycle Controller-Handbücher • Dell VMware-Dokumentation • Produktseite für OpenManage Integration for VMware vCenter • Dell Hilfs- und Supportstartseite • Dell TechCenter
Tipps für Support-Anrufe	Bietet Tipps an, wie Sie Dell Support kontaktieren und Anrufe richtig weiterleiten.
Fehlerbehebungsbündel	Laden Sie das Fehlerbehebungsbündel herunter. Stellen Sie dieses Bündel bereit oder verweisen Sie darauf, wenn Sie mit dem technischen Support Kontakt aufnehmen. Weitere Informationen finden Sie unter **Download a Troubleshooting Bundle**
Dell empfiehlt	Dell empfiehlt Dell Repository Manager, und Sie können hier einen Link dazu finden. Verwenden Sie Dell Repository Manager, um alle Firmware-Aktualisierungen, die für Ihr System verfügbar sind, zu finden und herunterzuladen.
iDRAC-Reset	Stellt eine Schaltfläche für das Reset von iDRAC bereit, die verwendet werden kann, wenn iDRAC nicht reagiert. Dieses Reset führt einen normalen Neustart von iDRAC aus. Siehe **Resetting iDRAC**

Herunterladen eines Fehlerbehebungsbündels

Verwenden Sie diese Informationen bei einer Fehlerbehebung oder senden Sie sie an den technischen Support.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
2. Klicken Sie auf **Erstellen und Herunterladen eines Fehlerbehebungsbündels**.
3. Klicken Sie auf die Schaltfläche **Erstellen**.
4. Klicken Sie auf **Speichern**, um die Datei zu speichern.
5. Klicken Sie im Dialog „Dateien herunterladen“ auf **Speichern**.
6. Wechseln Sie im Dialogfeld „Datei speichern“ in das Verzeichnis, in dem die Datei gespeichert werden soll, und klicken Sie auf **Speichern**.
7. Klicken Sie zum Beenden auf **Schließen**.

Soft iDRAC Reset

Sie können die Schaltfläche für das Reset von iDRAC auf der Registerkarte Hilfe und Support finden. Das Reset von iDRAC führt einen normalen iDRAC-Neustart durch. Der iDRAC-Neustart startet den Host nicht neu. Nach der Ausführung eines Reset dauert es bis zu 2 Minuten, zu einem verwendbaren Zustand zurückzukehren. Verwenden Sie diesen Reset nur in Fällen, in denen das iDRAC nicht in der OpenManage Integration for VMware vCenter reagiert.



ANMERKUNG: Dell empfiehlt, dass Sie den Host in den Wartungsmodus versetzen, bevor Sie ein Reset von iDRAC ausführen. Sie können diese Reset-Aktion nur auf einem Host ausführen, der Teil eines Verbindungsprofils ist, das mindestens einmal in einer Bestandsaufnahme aufgenommen wurde. Diese Reset-Aktion bringt den iDRAC evtl. nicht in einen verwendbaren Zustand zurück. In diesem Fall ist ein harter Reset erforderlich. Weitere Informationen über einen harten Reset finden Sie in Ihrer iDRAC-Dokumentation.

Während der Neustart des iDRACs durchgeführt wird, sehen Sie eventuell folgende Meldungen:

- Es ist eine Verzögerung oder ein Kommunikationsfehler aufgetreten, während OpenManage Integration for VMware vCenter seinen Funktionszustand abgerufen hat.
- Alle mit iDRAC geöffneten Sitzungen werden geschlossen.
- Die DHCP-Adresse für iDRAC könnte sich ändern.

  Falls iDRAC DHCP für seine IP-Adresse verwendet, dann besteht die Möglichkeit, dass die IP-Adresse sich ändert. Falls dies eintrifft, führen Sie den Host-Bestandsaufnahme-Job erneut aus, um die neue iDRAC-IP-Adresse in den Bestandsdaten zu erfassen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
2. Klicken Sie unter iDRAC Reset auf **Reset iDRAC**.
3. Geben Sie im iDRAC Reset-Dialog unter iDRAC Reset die Host-IP-Adresse/den -Namen ein.
4. Um zu bestätigen, dass Sie den iDRAC-Reset-Vorgang verstehen, wählen Sie **Ich verstehe den iDRAC-Reset. Weiter mit dem iDRAC-Reset**.
5. Klicken Sie auf **Reset iDRAC**.

Starten der Administrationskonsole

Stellen Sie OpenManage Integration for VMware vCenter OVF bereit, und registrieren Sie sich mit der VMware vCenter-Konsole, bevor Sie auf die Administrations-Konsole zugreifen. Lesen Sie das *OpenManage Integration for VMware vCenterSchnellstart-Handbuch*. Der Benutzername „admin“ ist der einzige erlaubte Benutzername und wird nach dem Import von OVF im Voraus erstellt. Sie müssen das Admin-Kennwort nach dem Import festlegen und es zur Anmeldung bei der Admin-Konsole verwenden.
Sie können OpenManage Integration for VMware vCenter von innerhalb des VMware vCenter-Webclient starten und die Administrationskonsole von der Registerkarte „Hilfe und Support“ aus öffnen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte „Hilfe und Support“ unter der Administrationskonsole auf den Link zur Konsole.
2. Verwenden Sie in der Administrationskonsolenanmeldng dasselbe Administratorkennwort, das Sie bei der Registrierung und der Einstellung des Admin-Benutzernamens und -Kennworts für OpenManage Integration for VMware vCenter verwendet haben. Unter Verwendung der Administrationskonsole können Sie Folgendes ausführen:
   a. Sie können ein vCenter registrieren oder seine Registrierung rückgängig machen, und Sie können Anmeldeinformationen ändern oder das Zertifikat aktualisieren.
   b. Sie können die Lizenz hochladen.
   c. Diese Seite enthält die Zusammenfassung über die Anzahl von registrierten und verfügbaren vCenters und über die Höchstzahl verwendeter und verfügbarer Hostlizenzen.
   d. Sie können das virtuelle Gerät neu starten.
   e. Aktualisieren (Upgrade auf die neueste Version ausführen).
   f. Fehlerbehebungsbündel erstellen.
   g. Zeigt die Netzwerkeinstellungen an (Nur-Lesen-Modus)
   h. Sie können die HTTP Proxy-Einstellungen konfigurieren: dies wird dazu verwendet, zum Geräte-Upgrade eine Verbindung mit dem Dell-Server zu erstellen oder für die Konnektivität mit ftp.dell.com
   i. Sie können NTP-Einstellungen konfigurieren, d. h. Sie können den NTP-Server aktivieren oder deaktivieren und bevorzugte und sekundäre NTP-Server konfigurieren
   j. Für HTTPS-Zertifikate können Sie eine Zertifikatsignierungsanforderung (CSR, certificate signing request) erstellen, ein Zertifikat hochladen oder das Standardzertifikat wiederherstellen.
   k. Konfigurieren Sie globale Einstellungen über die Art der Speicherung von Warnungen für alle vCenter-Instanzen. Sie können die maximale Anzahl der zu speichernden Warnungen, für wie viele Tage sie beibehalten werden sollen und die Zeitüberschreitung für duplizierte Warnungen konfigurieren.
   l. Sie können ein Backup oder eine Wiederherstellung einleiten.

m. Konfigurieren Sie den Backup-Standort auf einer Netzwerkfreigabe und das Verschlüsselungskennwort für die gesicherten Dateien (zusammen mit dem Test der Netzwerkverbindung).
n. Sie können wiederholte Backups planen.

4

Profile

Auf der Registerkarte „Anmeldeprofile“ können Sie die Verbindungsprofile und die Gehäuseprofile verwalten und konfigurieren.

Mit den Verbindungsprofilen können Sie Verbindungsprofile verwalten und konfigurieren, die für den Zugriff auf Dell-Server benötigt werden. Über das Fenster bzw. den Link für „Verbindungsprofil“ können Sie die Verbindungsprofile verwalten und konfigurieren, die die Anmeldeinformationen enthalten, die durch das virtuelle Gerät für die Kommunikation mit Dell-Servern verwendet werden. Ordnen Sie jedem Dell-Server nur ein Verbindungsprofil für die Verwaltung durch OpenManage Integration for VMware vCenter zu. Sie können einem einzelnen Verbindungsprofil mehrere Server zuweisen.

Mit den Gehäuseprofilen können Sie die Verbindungsprofile verwalten und konfigurieren, die die Anmeldeinformationen enthalten, die durch das virtuelle Gerät für die Kommunikation mit Dell-Gehäusen verwendet werden. Weisen Sie jedem erkannten Gehäuse ein Gehäuseprofil zur Verwaltung durch OpenManage Integration for VMware vCenter zu. Sie können einem einzigen Gehäuseprofil mehrere Gehäuse zuweisen.

Verbindungsprofile anzeigen

Bevor Sie es anzeigen können, müssen Sie ein Verbindungsprofil erstellen.
Nachdem Sie ein oder mehrere Profile erstellt haben, können Sie diese auf der Seite „Verbindungsprofil“ anzeigen.
OpenManage Integration for VMware vCenter verwendet Profile, um mit Dell-Hosts zu kommunizieren.

In OpenManage Integration for VMware vCenter auf der Seite **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** können Sie alle von Ihnen erstellten Verbindungsprofile anzeigen. Die Informationen, die Sie anzeigen können, umfassen:

Profilname Zeigt den Namen des Verbindungsprofils an.

Beschreibung Zeigt eine Beschreibung an, falls vorhanden.

vCenter Zeigt den vollständigen qualifizierten Domänennamen (FQDN) oder den Hostnamen oder aber die IP-Adresse des vCenter entsprechend dem Kontext an.

Zugeordnete Hosts Zeigt die Hosts an, die diesem Verbindungsprofil zugeordnet sind. Wenn es mehr als einen gibt, können sie das Erweiterungssymbol verwenden, um alle anzuzeigen.

iDRAC-Zertifikatsüberprüfung	Gibt an, ob die iDRAC-Zertifikatsüberprüfung aktiviert oder deaktiviert ist.
Host-Stamm-Zertifikatsüberprüfung	Gibt an, ob die Host-Stamm-Zertifikatsüberprüfung aktiviert oder deaktiviert ist.
Erstellungsdatum	Zeigt das Herstellungsdatum an.
Geändertes Datum	Zeigt das geänderte Datum an.
Zuletzt geändert von	Zeigt Einzelheiten zu einem Benutzer an.

Erstellen eines neuen Verbindungsprofils

Sie können einem einzelnen Verbindungsprofil mehrere Server zuweisen. Erstellen Sie ein Verbindungsprofil mit Hilfe der Registerkarte OpenManage Integration for VMware vCenter**Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile**, und klicken Sie zum Fortfahren auf das Plus-Zeichen.



ANMERKUNG: Die vCenter-Hosts, die während dieses Vorgangs angezeigt werden, wurden mit derselben Single Sign On (SSO) authentifiziert. Falls Sie keinen vCenter-Host sehen, befindet er sich evtl. auf einem anderen SSO, oder Sie verwenden eine VMware vCenter-Version unter 5.1.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofil** auf das Symbol **Neu erstellen**.
2. Klicken Sie auf der Seite **Verbindungsprofil – Willkommen** auf **Weiter**.
3. Führen Sie im Register **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Geben Sie unter „Profil“ den **Profilnamen** und optional eine **Beschreibung** ein.
   b. Wählen Sie unter vCenter den Host oder die Hosts aus, auf denen Sie dieses Verbindungsprofil zuweisen möchten. Mit dieser Option können Sie ein Verbindungsprofil für viele vCenter-Hosts erstellen.
   c. Verfahren Sie unter **iDRAC-Anmeldeinformationen** folgendermaßen:
      - Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.
      - Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domäne\Benutzername oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.
      - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
      - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
      - Führen Sie die folgenden Vorgänge aus:
        – Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
        – Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren** nicht.
   d. Führen Sie auf der Seite **Hosts-Root** folgendes aus:
      - Für Hosts, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um Ihre Host-Anmeldeinformationen zu konfigurieren.

        Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domäne\Benutzername oder benutzername@domäne. Der

Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.

- Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
- Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
- Führen Sie eine der folgenden Aktionen aus:
  - Aktivieren Sie das Kontrollkästchen , um das Host-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
  - Wenn Sie keine Prüfung ausführen und das Host-Zertifikat nicht speichern möchten, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren** nicht.
- Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:
- Im Textfeld ist der **Benutzername** root. Dies ist der Standardbenutzername, und Sie können den Benutzernamen nicht ändern.
- Falls das Active Directory eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, nicht nur root.
- Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

  ANMERKUNG: Der OMSA-Berechtigungsnachweis ist der gleiche, der auch für ESX- und ESXi-Hosts verwendet wird.

- Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
- Wählen Sie im Kontrollkästchen **Zertifikatprüfung aktivieren** eine der folgenden Optionen aus:
- Um das Host-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
- Wenn Sie keine Prüfung ausführen und das Host-Zertifikat nicht speichern möchten, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren** nicht.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite „Zugewiesene Hosts“ die Hosts für das Verbindungsprofil aus und klicken Sie auf **OK**.
6. Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus, und klicken dann auf die Schaltfläche „Verbindung testen“. Dieser Schritt ist optional. Er wird verwendet, um zu prüfen, ob der Host und die Host- und iDRAC-Anmeldeinformationen korrekt sind oder nicht.
7. Klicken Sie zum Vollenden des Profils auf **Weiter**. Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest „Für dieses System nicht anwendbar“.

Bearbeiten eines Verbindungsprofils

Nachdem Sie ein Verbindungsprofil konfiguriert haben, können Sie den Profilnamen, die Beschreibung, die zugeordneten Hosts und die Anmeldeinformationen bearbeiten.



ANMERKUNG: Die vCenters, die während dieses Vorgangs angezeigt werden, wurden unter Verwendung desselben Single Sign On (SSO) authentifiziert. Falls Sie keinen vCenter-Host sehen, befindet dieser sich evtl. auf einem anderen SSO oder Sie verwenden vielleicht eine VMware vCenter-Version unter 5.1.

ANMERKUNG: Sie können das Standardverbindungsprofil ungeachtet der Lizenzbeschränkung bearbeiten.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** ein Verbindungsprofil aus.
2. Klicken Sie auf das Symbol **Bearbeiten**.
3. Lesen Sie die Informationen im Fenster „Verbindungsprofil“ und klicken Sie auf **Weiter**.

4. Führen Sie im Register „Name und Speicherort“ folgende Schritte aus:
   a. Geben Sie unter „Profil“ den **Profilnamen** und optional eine **Beschreibung** ein.
   b. Zeigen Sie unter vCenter die zugeordneten Hosts für dieses Verbindungsprofil an. Sehen Sie den obigen Hinweis, warum Sie die Hosts hier angezeigt sehen.
   c. Verfahren Sie unter „iDRAC-Anmeldeinformationen“ folgendermaßen:

      - Der Standardbenutzername lautet root, und dieser Eintrag kann nicht geändert werden, wenn Sie nicht die Option **Active Directory** auswählen. Es ist nicht erforderlich, dass der iDRAC-Benutzer die root-Anmeldeinformationen verwendet, es kann sich um jeden Benutzer mit Administrator-Berechtigungen handeln, falls das **Active Directory** eingestellt ist.
      - Domäne\Benutzername: Geben Sie den Benutzernamen in einem dieser Formate ein: domäne \benutzername oder domäne@benutzername.

         **ANMERKUNG:** Die folgenden Zeichen sind für den Benutzernamen zulässig: / (Schrägstrich), &, \ (umgekehrter Schrägstrich), . (Punkt), " (Anführungszeichen), @, % (Prozent) (Begrenzung auf 127 Zeichen).

        Die Domain darf nur alphanumerische Zeichen enthalten und - (Bindestrich) und . (Punkt) (Begrenzung auf 254 Zeichen). Das erste und letzte Zeichen der Domain muss alphanumerisch sein.
      - Kennwort: Geben Sie Ihr Kennwort ein.

        Die folgenden Zeichen sind für das Kennwort nicht zulässig: / (Schrägstrich), &, \ (umgekehrter Schrägstrich), . (Punkt), " (Anführungszeichen).
      - Bestätigtes Kennwort: Geben Sie Ihr Kennwort noch einmal ein.
      - Zertifikatsüberprüfungen aktivieren: Die Standardeinstellung ist ein inaktives Kontrollkästchen. Wählen Sie zum Downloaden und Speichern des iDRAC-Zertifikats und dessen Prüfung während allen zukünftigen Verbindungen **Zertifikatsüberprüfungen aktivieren** aus, oder deaktivieren Sie das Kontrollkästchen **Zertifikatsüberprüfungen aktivieren**, um keine Zertifikatsüberprüfung durchzuführen und das Zertifikat nicht zu speichern.

        ANMERKUNG: Wenn Sie Active Directory verwenden, müssen Sie **Aktivieren** auswählen.
   d. Verfahren Sie unter „Host Root“ folgendermaßen:

      - Wählen Sie das Kontrollkästchen **Active Directory verwenden**, um auf alle, dem Active Directory zugeordneten, Konsolen zuzugreifen.

        Benutzername: Der Standardbenutzername ist **root** und kann nicht geändert werden. Falls „Active Directory verwenden“ ausgewählt ist, können Sie einen beliebigen Active Directory-Benutzernamen verwenden.
      - Kennwort: Geben Sie Ihr Kennwort ein.

        Die folgenden Zeichen sind für das Kennwort nicht zulässig: / (Schrägstrich), &, \ (umgekehrter Schrägstrich), . (Punkt), " (Anführungszeichen).
      - Bestätigtes Kennwort: Geben Sie Ihr Kennwort noch einmal ein.
      - Zertifikatsüberprüfungen aktivieren: Die Standardeinstellung ist ein inaktives Kontrollkästchen. Wählen Sie zum Downloaden und Speichern des iDRAC-Zertifikats und dessen Prüfung während allen zukünftigen Verbindungen **Zertifikatsüberprüfungen aktivieren** aus, oder deaktivieren Sie das Kontrollkästchen **Zertifikatsüberprüfungen aktivieren**, um keine Zertifikatsüberprüfung durchzuführen und das Zertifikat nicht zu speichern.

         **ANMERKUNG:** Wenn Sie Active Directory verwenden, müssen Sie **Aktivieren** auswählen.

    **ANMERKUNG:** Der OMSA-Berechtigungsnachweis ist der gleiche, der auch für ESX- und ESXi-Hosts verwendet wird.

ANMERKUNG: Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest *Für dieses System nicht anwendbar*.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie im Dialogfeld „Hosts auswählen“ die Hosts für dieses Verbindungsprofil aus.
7. Klicken Sie auf **OK**.
8. Mit der Registerkarte „Zugeordneter Host“ können Sie den iDRAC und die Host-Anmeldeinformationen auf den ausgewählten Servern testen. Hierbei sind folgende Möglichkeiten vorhanden:

   - Wählen Sie zum Beginnen des Tests die zu überprüfenden Hosts aus und klicken Sie auf das Symbol **Verbindung testen**. Die anderen Optionen sind inaktiv.

     Klicken Sie nach Abschluss des Tests auf **Fertigstellen**
   - Klicken Sie zum Stoppen der Tests auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld „Tests abbrechen“ auf **OK** und anschließend auf **Fertigstellen**.

Aktualisieren eines Verbindungsprofils

Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** oben in der Titelleiste des VMware vSphere Web Clients auf das Symbol **Aktualisieren**.



ANMERKUNG: Nach Entfernen des Hosts aus vCenter werden Sie zum Entfernen des Hosts aus dem Verbindungsprofil aufgefordert, wenn Sie auf die Seite Verbindungsprofil wechseln. Nach der Bestätigung wird der Host aus dem Verbindungsprofil entfernt.

Löschen eines Verbindungsprofils

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwaltung** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** und wählen Sie das Profil aus, das Sie löschen möchten.
2. Klicken Sie auf das **Löschen**-Symbol.
3. Klicken Sie in der Meldung „Löschen bestätigen“ zum Entfernen des Profils auf **Ja** oder klicken Sie auf **Nein**, um die Löschen-Aktion abzubrechen.

Testen eines Verbindungsprofils

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** ein zu testendes Verbindungsprofil aus. Diese Aktion kann einige Minuten in Anspruch nehmen.
2. Wählen Sie im Dialog „Verbindungsprofil testen“ die Hosts aus, die Sie testen wollen und klicken Sie anschließend auf das Symbol **Verbindung testen**.
3. Klicken Sie zum Abbrechen aller ausgewählter Tests und zum Beenden des Testens auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld „Tests abbrechen“ auf **OK**.
4. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Erstellen eines Gehäuse-Profils

Ein Gehäuse-Anmeldeinformationsprofil kann mit einem oder mehreren Gehäusen erstellt werden. Das Gehäuseprofil wird anhand der folgenden Schritte erstellt:

1. Wählen Sie in **OpenManage Integration** die Option **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Gehäuse-Profil** aus.

ANMERKUNG: Nach Ausführen der Host-Bestandsaufnahme wird das Gehäuse erkannt und für eine Zuordnung zum Gehäuse-Profil verfügbar.

2. Klicken Sie auf der Seite **Gehäuse-Profile** auf das Pluszeichen (+), um ein neues Gehäuse-Profil zu erstellen.
3. Führen Sie auf der Seite des **Gehäuse-Profil-Assistenten** die folgenden Schritte aus:

   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
4. Verfahren Sie unter **Anmeldeinformationen** folgendermaßen:

   - Geben Sie in das Textfeld **Benutzername** die Gehäuseanmeldeinformationen mit Administratorrechten ein, die in der Regel für die Anmeldung am Gehäuse verwendet werden.
   - Geben Sie in das Textfeld **Kennwort** das Kennwort ein, das Sie zur Anmeldung am Gehäuse verwenden.
   - Geben Sie im Textfeld **Kennwort überprüfen** dasselbe Kennwort ein, das Sie im Textfeld **Kennwort** eingegeben haben. Die Kennwörter müssen übereinstimmen.

   ANMERKUNG: Bei den Anmeldeinformationen kann es sich um lokale oder Active-Directory-Anmeldeinformationen handeln.
5. Klicken Sie auf **Weiter**. Die Seite **Gehäuse auswählen** wird angezeigt und zeigt alle inventarisierten Gehäuse für die Hosts an.
6. Um entweder ein einzelnes Gehäuse oder mehrere Gehäuse auszuwählen, wählen Sie die entsprechenden Kontrollkästchen neben der Spalte **IP/Host-Name** aus.

   Wenn das ausgewählte Gehäuse bereits Teil eines anderen Profils ist, wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass das ausgewählte Gehäuse einem Profil zugeordnet ist.

   Sie haben z. B. ein Profil **Test,** das Chassis A zugordnet ist. Wenn Sie ein anderes Profil, **Test 1,** erstellen und versuchen, eine Verbindung zwische Gehäuse A und **Test 1** herzustellen, wird eine Warnmeldung angezeigt.
7. Klicken Sie auf **OK**. Die Seite **Zugewiesene Gehäuse** wird angezeigt.
8. Wählen Sie das Gehäuse aus und klicken Sie auf das Symbol **Verbindung testen**, um die Konnektivität des Gehäuses zu testen, wobei die Anmeldeinformationen geprüft werden und das Ergebnis in der Spalte **Testergebnis** als **Bestanden** oder **Durchgefallen** angezeigt wird.
9. Klicken Sie auf **Fertig stellen**, um das Profil abzuschließen.

   ANMERKUNG: Sie können auch ein Gehäuse hinzufügen oder entfernen, indem Sie auf das Plus-Symbol klicken, das in der obersten Zeile der Seite **Zugeordnete Gehäuse** angezeigt wird.

Anzeigen von Gehäuse-Profilen

So zeigen Sie Gehäuse-Profile an:

1. Wählen Sie in der **OpenManage-Integration** das Fenster **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Gehäuse-Profile** aus. Die Gehäuseprofile werden angezeigt.
2. Wenn mehrere Gehäuse mit dem Chassis-Profil verbunden sind, werden durch das Klicken auf das Pfeilsymbol alle zugehörigen Gehäuse angezeigt.
3. Auf der Seite **Gehäuse-Ansicht** können Sie Profilnamen, Beschreibung, Gehäuse-IP, Service-Tag-Nummer sowie das Datum ansehen, an dem Sie das Gehäuse verändert haben.
4. Auf der Seite **Gehäuse-Ansicht** können Sie folgende Maßnahmen durchführen:
   a. Hinzufügen
   b. Bearbeiten
   c. Löschen
   d. Konnektivität testen

Bearbeiten eines Gehäuse-Profils

Nachdem Sie ein Gehäuse-Profil konfiguriert haben, können Sie den Profilnamen, die Beschreibung, die zugeordneten Gehäuse und die Anmeldeinformationen bearbeiten.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Verbindungsprofile** ein Gehäuseprofil aus.
2. Klicken Sie auf das Symbol **Bearbeiten** im Hauptmenü, das in Form eines schrägen **Pencil** (Bleistifts) angezeigt wird.
3. Die Fenster **Gehäuse-Profil bearbeiten** wird angezeigt.
4. Im Bereich **Gehäuse-Profil** können Sie den **Profilnamen** und eine optionale **Beschreibung** bearbeiten.
5. Unter dem Bereich **Anmeldeinformationen** können Sie den **Benutzernamen** und das **Kennwort** bearbeiten sowie das **Kennwort überprüfen**. Das Kennwort, das Sie im Feld **Kennwort überprüfen** eingeben, muss das gleiche wie das im Feld **Kennwort** eingegebene sein. Die eingegebenen Anmeldeinformationen müssen Administratorrechte am Gehäuse besitzen.
6. Klicken Sie auf **Anwenden**. Die Änderungen werden gespeichert.
7. Mit der Registerkarte **Zugeordnetes Gehäuse** können Sie das Gehäuse und die Anmeldeinformationen auf dem ausgewählten Gehäuse testen. Hierbei sind folgende Möglichkeiten vorhanden:

   - Um den Test zu beginnen, wählen Sie entweder ein einzelnes Gehäuse oder mehrere Gehäuse zum Prüfen aus und klicken Sie anschließend auf das Symbol **Verbindung testen**. Die Spalte **Testergebnis** zeigt an, ob die Testverbindung erfolgreich war oder nicht.
   - Sie können entweder ein oder mehrere Gehäuse löschen oder zu einem Gehäuse-Profil hinzufügen, indem Sie auf das **Plus**-Symbol klicken.

    **ANMERKUNG:** Wenn die Gehäuse nicht inventarisiert sind, werden nur IP/Host-Name und die Service-Tag-Nummer angezeigt. Die Felder **Gehäusename** und **Modell** werden angezeigt, sobald das Gehäuse inventarisiert ist.

Löschen von Gehäuse-Profilen

So löschen Sie Gehäuse-Profile:

1. Wählen Sie in der **OpenManage-Integration** das Fenster **Verwalten** → **Profile** → **Anmeldeinformationenprofil** → **Gehäuse-Profile** aus.
2. Wählen Sie ein Gehäuseprofil aus, das Sie löschen möchten, und klicken Sie auf das **Kreuz**-Symbol (X). Daraufhin wird ein Warnhinweis angezeigt.
3. Klicken Sie auf **Ja**, um den Löschvorgang fortzusetzen, oder klicken Sie auf **Nein**, um den Löschvorgang abzubrechen.

    **ANMERKUNG:** Wenn alle einem Gehäuseprofil zugeordneten Gehäuse abgewählt oder auf unterschiedliche Profile verschoben wurden, wird eine Bestätigungsmeldung über das Löschen angezeigt, die besagt, dass das Gehäuseprofil keine zugeordneten Gehäuse aufweist und gelöscht wird. Klicken Sie auf „OK“, um das Gehäuseprofil zu löschen.

Testen eines Gehäuse-Profils

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeinformationenprofile** → **Gehäuseprofile** ein einzelnes oder mehrere zu testende Gehäuse-Profile aus. Diese Aktion kann einige Minuten in Anspruch nehmen.
2. Wählen Sie im Dialog „Gehäuse-Profil testen“ das Gehäuse aus, das Sie testen möchten, und klicken Sie anschließend auf das Symbol **Verbindung testen**.

3. Klicken Sie zum Abbrechen aller ausgewählter Tests und zum Beenden des Testens auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld „Tests abbrechen“ auf **OK**.
4. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

5 Job-Warteschlange

Nach der Konfiguration von OpenManage Integration for VMware vCenter können Sie die Bestandsaufnahme, Garantie-Jobs und Firmwareaktualisierungen unter der Registerkarte „Überwachen“ überwachen. Die Bestandsaufnahme und Garantie werden mit dem Konfigurationsassistenten oder der Registerkarte „Einstellungen“ eingerichtet.

- Bestandsaufnahmenverlauf
- Garantieverlauf

Bestandsaufnahmenverlauf

Bestandaufnahme-Jobs werden unter Verwendung des Einstellungsregisters oder des Erstkonfigurationsassistenten eingerichtet. Verwenden Sie die Registerkarte „Bestandsaufnahmenverlauf“, um die Bestandsaufnahme-Jobs anzuzeigen. Sie können diese Tasks, von dieser Registerkarte aus durchführen:

- Anzeigen von Host-Bestand
- Bestandsaufnahme-Jobzeitpläne ändern
- Sofortige Ausführung eines Bestandsaufnahme-Jobs
- Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs

Anzeigen von Host-Bestandsaufnahmen

Zum Sammeln der Daten ist eine erfolgreich beendete Bestandsaufnahme erforderlich. Wenn die Bestandsaufnahme einmal beendet ist, können Sie die Bestandsaufnahmenergebnisse für das ganze Datacenter oder für ein einzelnes Hostsystem anzeigen. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs. Die Spalten sind in aufsteigender und absteigender Reihenfolge sortierbar.

Wenn Serverdaten weder abgerufen noch angezeigt werden können, gibt es mehrere mögliche Ursachen:

- Dem Server wurde kein Verbindungsprofil zugeordnet, weswegen kein Bestandsaufnahme-Job durchgeführt werden kann.
- Es wurde kein Bestandsaufnahme-Job auf dem Server ausgeführt, um die Daten zu erfassen. Somit können keine Daten angezeigt werden.
- Die Anzahl der Hostlizenzen wurde überschritten. Sie müssen zusätzliche Lizenzen erwerben, um den Bestandsaufnahme-Job vollständig abschließen zu können.
- Der Server verfügt nicht über die erforderliche iDRAC-Lizenz für Server der 12. Generation von Dell PowerEdge-Servern und später, und Sie müssen die korrekte iDRAC-Lizenz erwerben.
- Anmeldeinformationen können möglicherweise falsch sein

- Ziel ist möglicherweise nicht erreichbar

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Überwachen**.
2. Klicken Sie auf **Job-Warteschlange** → **Bestandsaufnahmenverlauf** → **Host-Bestandsaufnahme.**
3. Wählen Sie zur Anzeige der Serverinformationen auf einem ausgewählten vCenter ein vCenter aus, um alle zugeordneten Host-Details anzuzeigen.
4. Überprüfen Sie die Host-Bestandslisteninformationen.

vCenter-Details	
Schaltfläche „Zeitplan ändern“	Zum Bearbeiten eines Bestandsaufnahmen-Zeitplans klicken.
Schaltfläche „Jetzt ausführen“	So führen Sie eine Bestandsaufnahme durch:
vCenter	Zeigt die vCenter-Adresse an.
Bestandene Hosts	Zeigt alle ausgefallenen Hosts an.
Nächste Bestandsaufnahme	Zeigt den nächsten auszuführenden Bestandsaufnahmenzeitplan an.
Letzte Bestandsaufnahme	Zeigt den zuletzt ausgeführten Bestandsaufnahmenzeitplan an.
Hosts	
Host	Zeigt die Host-Adresse an.
Status	Zeigt den Status an. Die Optionen beinhalten: • Erfolgreich • Fehlgeschlagen • Wird durchgeführt • Geplant
Dauer (MM:SS)	Zeigt die Dauer des Jobs in Minuten und Sekunden an.
Startdatum und -uhrzeit	Zeigt den Datum und die Uhrzeit an, zu dem der Bestandsaufnahmenzeitplan gestartet wurde.
Enddatum und -zeit	Zeigt die Uhrzeit des Endes des Bestandsaufnahmenzeitplans an.

Bestandsaufnahme-Jobzeitpläne ändern

Um sicherzustellen, dass die Serverinformationen auf dem neuesten Stand sind, müssen Sie auf Dell-Servern in regelmäßigen Abständen Bestandsaufnahmen durchführen. Dell empfiehlt, einmal pro Woche eine Bestandsaufnahme durchzuführen. Bestandsaufnahmen haben keinen Einfluss auf die Leistung des Hosts. Sie können einen Bestandsaufnahme-Jobzeitplan auf der Seite **Überwachen** → **Job-Warteschlange** → **Bestandsaufnahmenverlauf** → **Host-Bestandsaufnahme** oder von der Seite **Verwalten** → **Einstellungen** aus durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Überwachen** → **Job-Warteschlange** auf**Bestandsaufnahmeverlauf** → **Host-Bestandsaufnahme**.
2. Wählen Sie ein vCenter aus und klicken Sie anschließend auf das Symbol **Zeitplan ändern**.
3. Führen Sie im Dialogfeld „Abruf von Bestandsaufnahmedaten“ folgendes durch:

a. Wählen Sie unter „Bestandsaufnahmedaten“ das Kontrollkästchen **Bestandsaufnahme-Datenabruf aktivieren** aus.
b. Wählen Sie unter „Datenabrufzeitpläne für Bestandsaufnahme“ die Wochentage für den Job aus.
c. Geben Sie im Textfeld „Uhrzeit für Bestandsaufnahme-Datenabruf“ die Ortszeit für diesen Job ein.

   Möglicherweise müssen Sie den Zeitunterschied zwischen Job-Konfiguration und Job-Umsetzung in Erwägung ziehen.

4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern, auf **Löschen**, um die Einstellungen neu einzustellen, und auf **Abbrechen**, um den Vorgang abzubrechen.

Sofortige Ausführung eines Bestandsaufnahme-Jobs

Führt und löst sofort einen Bestandsaufnahme-Task für das ausgewählten VCenter aus.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Überwachen** → **Job-Warteschlange** auf **Bestandsaufnahmenverlauf** → **Host-Bestandsaufnahme**.
2. Klicken Sie auf die Schaltfläche **Jetzt ausführen**.
3. Klicken Sie im Dialogfeld „Erfolgreich“ auf **Schließen**.



ANMERKUNG: Beim Ausführen einer modularen Host-Bestandsaufnahme werden entsprechende Gehäuse automatisch erkannt.

Ein Bestandsaufnahme-Job steht nun in der Warteschlange. Beachten Sie, dass Sie keine Bestandsaufnahme für einen einzelnen Host ausführen können. Ein Bestandsaufnahme-Job startet für alle Hosts.

Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs

Sie können auf der Registerkarte **Gehäuse-Bestandsaufnahme** einen Gehäuse-Bestandsaufnahme-Job anzeigen und durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Überwachen** → **Job-Warteschlange** auf **Bestandsaufnahmenverlauf** → **Gehäuse-Bestandsaufnahme**.
2. Die Liste von Gehäusen und der Status, dass bei der letzten Ausführung der Bestandsliste eine Bestandsaufnahme durchgeführt wurde, wird angezeigt.

   ANMERKUNG: Die geplante Gehäuse-Bestandsaufnahme wird zur selben Zeit durchgeführt wie die geplante Host-Bestandsaufnahme.

3. Klicken Sie auf die Schaltfläche **Jetzt ausführen**. Daraufhin werden die Listen aktualisierter inventarisierter Gehäuse für jedes Gehäuse mit dem Status **Erfolgreich** oder **Fehlgeschlagen** angezeigt.

Garantieverlauf

Hardware-Garantieinformationen werden von Dell Online abgerufen und von OpenManage Integration for VMware vCenter angezeigt. Die Service-Tag-Nummer wird zur Sammlung von Garantieinformationen über den Server verwendet. Abfrage-Jobs für Garantiedaten werden unter Verwendung des Konfigurationsassistenten eingerichtet. Zeigen Sie den Verlauf des Garantie-Jobs auf dieser Registerkarte an. Zu den auf dieser Registerkarte durchführbaren Tasks gehört Folgendes:

- Anzeigen des Garantieverlaufs
- Ändern eines Garantie-Jobzeitplans
- Sofortiges Ausführen eines Garantie-Jobs

Anzeigen des Garantieverlaufs

Ein Garantie-Job ist ein geplanter Task zum Abrufen von Garantieinformationen auf allen Systemen von dell.com/support. Spalten sind in aufsteigender und absteigender Reihenfolge sortierbar.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Überwachen**.
2. Klicken Sie auf **Job-Warteschlange** → **Garantieverlauf.**
3. Erweitern Sie die den Garantieverlauf, um die **Host-Garantie** und die **Gehäusegarantie** anzuzeigen.
4. Wählen Sie entweder **Host-Garantie** oder **Gehäusegarantie** aus, um die entsprechenden Informationen zum Garantie-Job-Verlauf anzusehen.

Schaltfläche zum Bearbeiten des Zeitplans	Zum Bearbeiten eines Garantie-Job-Zeitplans anklicken.
Schaltfläche „Jetzt ausführen“	Klicken Sie, um einen Garantie-Job auszuführen.
vCenter-Verlauf	
vCenter	Anzeigen von vCenter-Listen.
Bestandene Hosts	Zeigt die Anzahl der vCenter-Hosts an, die bestanden haben.
Letzte Garantie	Zeigt den zuletzt ausgeführten Garantie-Job an.
Nächste Garantie	Zeigt den nächsten auszuführenden Garantie-Job an.
Hosts-Verlauf	
Host	Zeigt die Host-Adresse an.
Status	Zeigt den Status an. Die Optionen beinhalten: • Erfolgreich • Fehlgeschlagen • Wird durchgeführt • Geplant
Dauer (MM:SS)	Zeigt die Dauer des Garantie-Jobs in MM:SS an.
Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu der der Garantie-Job gestartet wurde.
Enddatum und -zeit	Zeigt die Uhrzeit an, zu der der Garantie-Job beendet wurde.
Gehäusehistorie	
Gehäuse-IP-Adresse	Zeigt die IP-Adresse des Gehäuses an.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer im Falle von Fragen und Wartungsdiensten.
Status	Zeigt den Status des Gehäuses an.
Dauer (MM:SS)	Zeigt die Dauer des Garantie-Jobs in MM:SS an.

Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu der der Garantie-Job gestartet wurde.
Enddatum und -zeit	Zeigt die Uhrzeit an, zu der der Garantie-Job beendet wurde.

Ändern eines Garantie-Jobzeitplans

Garantie-Job werden ursprünglich im Erstkonfigurationsassistenten konfiguriert. Sie können den Zeitplan für einen Garantie-Job über die Seite **Überwachen (Registerkarte)** → **Job-Warteschlange** → **Garantieverlauf** → **Host-Garantie**oder über die Seite **Verwalten (Registerkarte)** → **Einstellungen** ändern.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf dem Register **Überwachen** → **Job-Warteschlange** auf **Garantieverlauf**.
2. Klicken Sie auf das Symbol **Zeitplan ändern**.
3. Führen Sie im Dialogfeld „Abruf von Garantiedaten“ folgendes durch:
   a. Wählen Sie unter „Garantiedaten“ das Kontrollkästchen **Garantiedatenabruf aktivieren** aus.
   b. Wählen Sie unter „Garantieabrufzeitplan“ die Wochentage für den Job aus.
   c. Geben Sie in den Textfeldern „Uhrzeit für Garantiedatenabruf“ die Ortszeit für diesen Job ein.
   Möglicherweise ist es erforderlich, dass Sie für die Ausführung dieses Jobs zur richtigen Uhrzeit einen Zeitunterschied berechnen.
4. Klicken Sie auf **Anwenden**.

Sofortiges Ausführen eines Host-Garantie-Jobs

Führen Sie mindestens einmal in der Woche einen Garantie-Job aus.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen** → **Job-Warteschlange.**
2. Klicken Sie auf **Garantieverlauf** und **Host-Garantie**, um den Garantie-Job auszuwählen, den Sie ausführen möchten.
3. Klicken Sie auf die Schaltfläche **Jetzt ausführen**.
4. Klicken Sie im Dialogfeld „Erfolgreich“ auf **Schließen**.



ANMERKUNG: Die Gehäusegarantie wird automatisch für alle Gehäuse ausgeführt, sobald die Host-Garantie ausgeführt wird. In einer SSO-Umgebung mit mehreren vCentern wird die Gehäusegarantie automatisch bei jedem vCenter ausgeführt, wenn die Garantie für ein beliebiges vCenter manuell ausgeführt wird.

Es befindet sich nun ein Garantie-Job in der Warteschlange.

Sofortiges Ausführen eines Gehäusegarantie-Jobs

Führen Sie mindestens einmal in der Woche einen Garantie-Job aus.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen** → **Job-Warteschlange**.
2. Klicken Sie auf **Garantieverlauf** und **Gehäusegarantie**, um den Garantie-Job auszuwählen, den Sie ausführen möchten.
3. Klicken Sie auf die Schaltfläche **Jetzt ausführen**.
4. Klicken Sie im Dialogfeld „Erfolgreich“ auf **Schließen**.
   Es befindet sich nun ein Garantie-Job in der Warteschlange.

Info über Protokolle

Sie können Benutzeraktionen auf der Registerkarte **Überwachen** → **Protokoll** von OpenManage Integration for VMware vCenter ansehen.

Sie können den Inhalt auf dieser Seite anhand der zwei Dropdown-Listen sortieren. Mit der ersten Dropdown-Liste können Sie der Dateikategorie nach sortieren. Dazu gehören die folgenden Kategorien:

- Alle Kategorien
- Info
- Warnung
- Fehler

Mit der zweiten Dropdown-Liste können Sie Zeitblöcken nach sortieren. Dazu gehören:

- Letzte Woche
- Letzten Monat
- Letztes Jahr
- Benutzerdefinierter Bereich

  Falls Sie einen benutzerdefinierten Bereich auswählen, können Sie das Start- und Enddatum auswählen und klicken Sie dann auf Anwenden.

Sie können die Datenrasterspalten auch in auf- oder absteigender Reihenfolge sortieren, indem Sie auf die Spaltenüberschrift klicken.

Verwenden Sie das Filtertextfeld, um in Ihrem Inhalt zu suchen.

Unter auf dem Seitenraster werden folgende Informationen angezeigt:

Elemente insgesamt	Zeigt die Gesamtzahl aller Protokollelemente an.
Elemente pro Bildschirm	Zeigt die Anzahl von Protokollelementen auf der angezeigten Seite an. Verwenden Sie das Dropdown-Feld, um die Anzahl der Elemente pro Seite einzustellen.
Seite	Zeigt die Seite an, auf der Sie sich befinden. Geben Sie eine Seitennummer im Textfeld ein oder verwenden Sie die Schaltflächen „Vorherig" und „Nächste", um zur gewünschten Seite zu gelangen.
Schaltflächen „Vorherig" oder „Nächste"	Schaltflächen, die Sie zu den nächsten oder vorherigen Seiten bringen.
Symbol „Alle exportieren"	Verwenden Sie dies, um den Protokollinhalt in eine CSV-Datei zu exportieren.

Anzeigen der Protokolle

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Überwachen**.
2. Sehen Sie auf dem Register „Protokoll" die Benutzermaßnahmenprotokolle für die OpenManage Integration for VMware vCenter an. Die Protokollseite zeigt Folgendes an:

Alle Kategorien	Ermöglicht Ihnen, die Protokolle auf Basis der folgenden Protokolltypen zu filtern und anzuzeigen: • Alle Kategorien

	• Info • Warnung • Fehler
Datumsfilter	Ermöglicht Ihnen, Protokolle nach den folgenden Daten zu filtern und anzuzeigen: • Letzte Woche • Letzten Monat • Letztes Jahr • Benutzerdefinierter Bereich Um das Datum auf Basis des bestimmten Datums zu filtern, wählen Sie die Option **Benutzerdefinierter Bereich** aus der Drop-Down-Liste für das Datum aus, anschließend geben Sie das **Startdatum** und das **Enddatum** ein, die als Grundlage für das Filtern dienen sollen, und klicken Sie anschließend auf **Anwenden**.
Suchen	Ermöglicht Ihnen auf Basis der Protokollbeschreibung oder eines bestimmten Textes im Protokoll zu filtern.
Kategorie	Zeigt den Kategorietyp an.
Datum und Uhrzeit	Zeigt das Datum und die Zeit der Benutzermaßnahme an.
Beschreibung	Zeigt eine Beschreibung der Benutzermaßnahme an.

3. Klicken Sie auf die Spaltenüberschrift, um die Daten im Gitter zu sortieren.
4. Um nach Kategorien oder Zeitblöcken zu sortieren, verwenden Sie die Dropdown-Listen oberhalb des Gitters.
5. Um zwischen den Seiten von Protokollelementen hin und her zu blättern, verwenden Sie die Schaltflächen „Vorhergehend“ und „Weiter“.

Protokolldateien exportieren

OpenManage Integration for VMware vCenter verwendet das CSV-Dateiformat (durch Komma getrennte Werte) für das Exportieren von Informationen aus Datentabellen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Zeigen Sie auf der Registerkarte „Protokoll“ die Benutzeraktionen für OpenManage Integration for VMware vCenter an.
3. Klicken Sie zum Exportieren einer Protokolldatei mit CSV-Formatierung in der rechten unteren Ecke des Bildschirms auf die Schaltfläche **Alle exportieren**.
4. Suchen Sie im Dialogfeld **Speicherort für Download auswählen** den Speicherort zum Speichern der Protokollinformationen.
5. Akzeptieren Sie im Textfeld **Dateiname** entweder den Standardnamen „ExportList.csv“, oder geben Sie Ihren eigenen Dateinamen ein.
6. Klicken Sie auf **Speichern**.

6

Konsolenverwaltung

Die Verwaltung des OpenManage Integration for VMware vCenter und dessen virtueller Umgebung wird mithilfe zweier zusätzlicher Administrator-Portale erreicht:

- Web-basierte Administration Console
- Konsolenansicht für einen bestimmten Server (die Konsole der virtuellen Maschine des Geräts).

Über diese beiden Portale können globale Einstellungen für die Verwaltung von vCenter, Backup und Wiederherstellung der OpenManage Integration for VMware vCenter-Datenbank sowie Aktionen zum Zurücksetzen/Neustart eingegeben und für alle vCenter-Instanzen verwendet werden.

Verwenden der Verwaltungskonsole

Im Fenster „vCenter Registration“ in der Verwaltungskonsole können Sie einen vCenter-Server registrieren und eine Lizenz hochladen oder erwerben. Wenn Sie eine Demolizenz verwenden, wird der Link „Software kaufen“ angezeigt, über den Sie eine vollständige Produktversion erwerben können, um mehrere Hosts zu verwalten. In diesem Abschnitt können Sie auch einen Server modifizieren, aktualisieren und die Registrierung aufheben.

Verwandte Aufgaben:

- Registrieren eines vCenter-Servers
  - Modifizieren der Administrator vCenter-Anmeldung
  - Aktualisieren der SSL-Zertifikate für registrierte vCenter
  - Deinstallieren von OpenManage Integration for VMware vCenter von vCenter
- Hochladen einer OpenManage Integration for VMware vCenter-Lizenz

Registrieren eines vCenter-Servers

Sie können OpenManage Integration für VMware vCenter nach der Installation von OpenManage Integration for VMware vCenter registrieren. OpenManage Integration for VMware vCenter verwendet das Admin-Benutzerkonto für vCenter-Vorgänge. OpenManage Integration for VMware vCenter unterstützt 10 vCenters pro Gerät.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie zum Registrieren eines neuen Servers im linken Fensterbereich auf **VCENTER REGISTRIERUNG** und dann auf **Neuen vCenter-Server registrieren**.
4. Führen Sie im Dialogfeld **Neues vCenter registrieren** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder ein FQDN des Hosts in das Textfeld **vCenter-Server-IP-Adresse oder Hostname** ein.
   b. Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
5. Unter **Admin-Benutzerkonto** führen Sie die folgenden Schritte aus:

a. Geben Sie den Benutzernamen des Administrators in das Textfeld **Admin-Benutzername** ein.
b. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
c. Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.

6. Klicken Sie auf **Registrieren**.

Anforderungen für OpenManage Integration for VMware vCenter

Die OpenManage Integration for VMware vCenter (OMIVV) erfordert Informationen von OpenManage auf Servern einer älteren Generation und neuere Plattformen sind darauf beschränkt, mit der Version von vSphere zu starten, die den neueren Chipsatz versteht. Daher gibt es Beschränkungen in Bezug auf die Version von vSphere, mit der eine bestimmte Version von OMIVV arbeitet.

ESXi-Versionen, die auf verwalteten Hosts unterstützt werden sollten:

ESX/ESXi-Version-Unterstützung	Plattform-Generation-Support				
	9G	10G	11G	12G	13G
v4.1 (ESX/ESXi)	J	J	J	N	N
v4.1 U1 (ESX/ESXi)	J	J	J	N	N
v4.1 U2 (ESX/ESXi)	J	J	J	J	N
v4.1 U3 (ESX/ESXi)	J	J	J	J	N
v5.0	J	J	J	J	N
v5.0 U1	J	J	J	J	N
v5.0 U2	J	J	J	J	N
v5.0 U3	J	J	J	J	N
v5.1	J	J	J	J	N
v5.1 U1	J	J	J	J	N
v5.1 U2	J	J	J	J	N
v5.5	N	j	J	J	N
v5.5 U1	N	N	N	N	J
v5.5 U2	N	N	N	J	J

vCenter sSupport

Derzeit ist die Unterstützung für v5.5 U1 nur mit Servern der 12. Generation über iDRAC mit Lifecycle Controller-Unterstützung verfügbar. OpenManage-Support für 5.5 U1 mit Servern der älteren Generation ist in Kürze zu erwarten. vSphere v5.5 U1 wird mit dem aktuellen Chipsatz nicht unterstützt, so wird es auf den Plattformen der 13. Generation auch nicht unterstützt.

Unterstützung für vSphere v5.5 U2

Mit der Unterstützung von iDRAC mit Lifecycle Controller 5.5 U2 wird vSphere für Plattformen der 12. und 13. Generation unterstützt.

Unterstützte vCenter Server-Versionen für Version 2.3

Die OpenManage Integration for VMware vCenter arbeitet mit jeder dieser vCenter Server-Versionen:

vCenter-Version	Desktop-Client-Support	Web-Client-Support
v5.0 U3	J	N
5.1 U2	J	N
v5.5	J	J
v5.5 U1	J	J
v5.5 U2	J	J

Mit jeder gegebenen vCenter-Version müssen die ESX / ESXi-Hosts, die es verwaltet, über eine gleiche oder niedrigere Version verfügen. Um eine vSphere v4.1- oder v5.0-Umgebung mit OMIVV zu verwalten, müssen Sie über eine vCenter-Mindestversion v5.0 U3 verfügen.

Modifizieren der vCenter Administrator-Anmeldung

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden im rechten Fensterbereich angezeigt. Klicken Sie zum Öffnen des Fensters **Admin-Konto modifizieren** unter **Anmeldeinformationen** auf **Modifizieren**.
4. Geben Sie den **Benutzername** und das **Kennwort** für den vCenter Administrator ein, und bestätigen Sie das Kennwort unter **Kennwort bestätigen**.
5. Klicken Sie auf **Anwenden**, um das Kennwort zu ändern, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren der SSL-Zertifikate für registrierte vCenter-Server

Wenn das SSL-Zertifikat auf einem vCenter-Server geändert wird, führen Sie die folgenden Schritte aus, um das neue Zertifikat für das OpenManage Integration for VMware vCenter zu importieren. DasOpenManage Integration for VMware vCenterr verwendet dieses Zertifikat, um sicherzustellen, dass der vCenter-Server mit dem richtigen vCenter-Server und nicht mit einem Nachahmer kommuniziert.

OpenManage Integration for VMware vCenter verwendet das openssl API zum Erstellen des Certificate Signing Request (CSR) unter Verwendung des RSA-Verschlüsselungsstandards mit einer 2048 Bitschlüssellänge. Das durch OpenManage Integration for VMware vCenter erstellte CRS erhält ein digital signiertes Zertifikat einer vertrauenswürdigen Zertifizierungsstelle. Das OpenManage Integration for VMware vCenter verwendet das digitale Zertifikat zum Aktivieren von SSL auf dem Webserver für eine sichere Kommunikation.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAdrdress> ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenters werden im rechten Fensterbereich angezeigt. Zur Aktualisierung der Zertifikate klicken Sie auf **Aktualisieren**.

Deinstallieren des OpenManage Integration for VMware vCenter von VMware vCenter

Um das OpenManage Integration for VMware vCenter zu entfernen, müssen Sie die Registrierung des vCenter-Servers unter Verwendung der Administrationskonsole aufheben.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.

3. Heben Sie auf der Seite **vCenter Registrierung** unter der vCenter-Server-Tabelle die Registrierung der OpenManage Integration for VMware vCenter durch das Klicken auf **Registrierung aufheben** auf.

   Wenn Sie mit mehreren vCentern arbeiten, achten Sie darauf, das richtige auszuwählen.
4. Wenn Sie im Dialogfeld **vCenter-Registrierung aufheben** gefragt werden, ob Sie die Registrierung dieses Servers aufheben möchten, klicken Sie auf **Registrierung aufheben**.

Hochladen einer OpenManage Integration for VMware vCenter-Lizenz auf die Administrationskonsole

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden in einer Tabelle angezeigt. Klicken Sie zum Anzeigen des Dialogfelds „Lizenz hochladen“ auf **Lizenz hochladen**.
4. Um zur Lizenzdatei zu navigieren, klicken Sie auf die Schaltfläche **Durchsuchen** und dann auf **Hochladen**.

   ANMERKUNG: Falls die Lizenzdatei irgendwie geändert oder bearbeitet wurde, sieht das Gerät sie als korrupt an, und die Datei funktioniert nicht. Sie können Lizenzen hinzufügen, wenn Sie mehr Hosts hinzufügen müssen. Befolgen Sie den obigen Vorgang, um weitere Lizenzen hinzuzufügen.

   ANMERKUNG: Wenn die Anzahl der erfolgreich inventarisierten Server der 11., 12. und 13. Generation der Anzahl der erworbenen Lizenzen entspricht, wird das Hinzufügen von Servern der 9. und 10. Generation zu neuen oder vorhandenen Verbindungsprofilen blockiert. Bearbeiten Sie vorhandene Verbindungsprofile, indem Sie einige Server der 11., 12., 13. Generation entfernen und stattdessen Server der 9. oder 10. Generation hinzufügen. Erstellen Sie ein neues Verbindungsprofil für die entfernten Server der 11., 12. oder 13. Generation.

Verwalten des virtuellen Geräts

Die Verwaltung des virtuellen Geräts beinhaltet die Informationen über das OpenManage Integration for VMware vCenter Netzwerk, Version, NTP und HTTPS-Informationen. Außerdem können Sie:

- Das virtuelle Gerät neustarten
- Das virtuelle Gerät aktualisieren und einen Speicherort für die Repository-Aktualisierung konfigurieren
- Ein Bündel für die Fehlerbehebung herunterladen
- Den NTP-Server einrichten
- HTTPS-Zertifikate hochladen

Neustarten des virtuellen Geräts

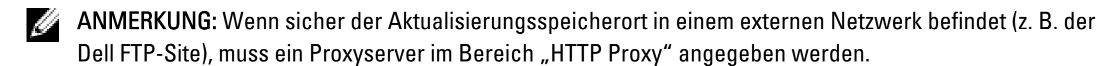
Das Neustarten des virtuellen Gerät meldet Sie von der Administration Console ab und das OpenManage Integration for VMware vCenter ist nicht mehr verfügbar, bis das virtuelle Gerät und seine Dienste aktiv sind.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Zu Neustart des OpenManage Integration for VMware vCenter klicken Sie auf **Neustarten des virtuellen Geräts**.
5. Klicken Sie im Dialogfeld **Virtuelles Gerät neustarten** auf **Anwenden**, um das virtuelle Gerät neu zu starten, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren eines Repository-Speicherorts und virtuellen Geräts

Führen Sie vor dem Aktualisieren des virtuelle Geräts ein Backup aus, um sicherzustellen, dass alle Daten geschützt sind. Siehe Verwalten von Backups und Wiederherstellungen.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie neben „Geräteaktualisierung" auf **Bearbeiten**.
5. Im Fenster **Geräteaktualisierung** geben Sie die **Repository-Standort URL** ein und klicken Sie auf **Anwenden**.



ANMERKUNG: Wenn sicher der Aktualisierungsspeicherort in einem externen Netzwerk befindet (z. B. der Dell FTP-Site), muss ein Proxyserver im Bereich „HTTP Proxy" angegeben werden.

Aktualisieren der Softwareversion des virtuellen Geräts

Erstellen Sie vor der Softwareaktualisierung ein Backup der Daten auf dem virtuellen Gerät, um einen möglichen Datenverlust vermeiden.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEWARTUNG**.
3. Klicken Sie zum Aktualisieren der Softwareversion des virtuellen Geräts unter **Geräteaktualisierung** auf **Virtuelles Gerät aktualisieren**.
4. Im Dialogfeld **Gerät aktualisieren** werden die aktuelle und die verfügbare Versionen aufgeführt. Klicken Sie auf **Aktualisieren**, um die Aktualisierung zu beginnen.
5. Das System wird gesperrt und in den Wartungsmodus versetzt. Nachdem die Aktualisierung abgeschlossen ist, zeigt die Seite „Gerät" die neu installierte Version an.

Herunterladen des Fehlerbehebungsbündels

Verwenden Sie diese Informationen bei einer Fehlerbehebung oder senden Sie sie an den technischen Support.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
3. Klicken Sie auf **Bündel für Fehlerbehebung erstellen**, um das Dialogfeld „Bündel für Fehlerbehebung" anzuzeigen.
4. Klicken Sie auf den Link **Bündel für Fehlerbehebung herunterladen**, um die Zip-Datei mit den Anmeldeinformationen für das virtuelle Gerät entweder zu öffnen oder zu speichern.
5. Klicken Sie zum Beenden auf **Schließen**.

Einrichten des HTTP-Proxy

Sie können die HTTP-Proxy-Einstellungen entweder in der Administrator Console oder in der Dell Management Console einrichten.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Scrollen Sie auf der Seite **Geräteverwaltung** bis zu **HTTP-Proxy-Einstellungen** und klicken Sie dann auf **Bearbeiten**.

5. Führen Sie auf der Seite **Bearbeiten** die folgenden Schritte aus:
   a. Wählen Sie neben **HTTP-Proxy-Einstellungen verwenden** die Option **Aktivieren**.
   b. Geben Sie die Proxyserver-Adresse in das Textfeld **Proxyserver-Adresse** ein.
   c. Geben Sie den Proxyserver-Port in das Textfeld **Proxyserver-Schnittstelle** ein.
   d. Wählen Sie neben **Proxy-Anmeldeinformationsnachweis verwenden** die Option **Ja**, um die Proxy-Anmeldeinformationen zu verwenden.
   e. Wenn Sie ie Anmeldeinformationen verwenden, geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   f. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
6. Klicken Sie auf **Anwenden**.

Einrichten der NTP-Server

Verwenden Sie das Network Time Protocol (NTP) zum Synchronisieren der Uhren der virtuellen Geräte mit der Uhr eines NTP-Servers.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung“ in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Für NTP bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen **Aktiviert**. Geben Sie den **Hostnamen** oder die **IP-Adresse** für einen **bevorzugten** und einen **sekundären NTP-Server** ein und klicken Sie auf **Anwenden**.
6. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Erzeugen einer Zertifikatsignierungsanforderung



ANMERKUNG: Sie müssen das Zertifikat vor der Registrierung des OpenManage Integration for VMware vCenter mit vCenter hochladen.

Das Erzeugen einer Zertifikatsignierungsanforderung verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikatsignierungsanforderung für HTTPS-Zertifikate erzeugen**. Eine Meldung zeigt an, dass wenn eine neue Anforderung erzeugt wird, mit dem vorherigen CSR erzeugte Zertifikate nicht mehr auf das Gerät hochgeladen werden. Klicken Sie zum Fortsetzen der Anforderung auf **Weiter**, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.
5. Geben Sie den **Allgemeinen Namen**,**Name der Organisation**, **Organisationseinheit**, **Standort**, **Name des Bundeslands/der Provinz**, **Land** und **E-Mail-Adresse** für die Anforderung ein. Klicken Sie dann auf **Fortsetzen**.
6. Klicken Sie auf **Herunterladen**, dann speichern Sie das resultierende HTTPS-Zertifikat an einem zugänglichen Speicherort.

Hochladen eines HTTPS-Zertifikats

HTTPS-Zertifikate werden für die sichere Kommunikation zwischen dem virtuellen Gerät und Hostsystemen verwendet. Um diese sichere Kommunikation einzurichten, muss eine Zertifikatssignierungsanfrage an eine Zertifizierungsstelle gesendet werden, dann wird das resultierende Zertifikat mithilfe der Administration Console hochgeladen. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

ANMERKUNG: Sie können entweder Microsoft Internet Explorer, Firefox oder Chrome verwenden, um Zertifikate hochzuladen.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikat für HTTPS-Zertifikate hochladen**.
5. Klicken Sie im Dialogfeld **Zertifikate hochladen** auf **OK**.
6. Klicken Sie zum Auswählen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
7. Klicken Sie auf **Abbrechen**, wenn Sie das Hochladen abbrechen müssen.

   ANMERKUNG: Das Zertifikat muss im PEM-Format vorliegen.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats

ANMERKUNG: Wenn Sie ein benutzerdefiniertes Zertifikat für Ihr Gerät hochladen möchten, müssen Sie das neue Zertifikat vor der Registrierung von vCenter hochladen. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden Kommunikationsfehler im Web-Client angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung aufheben und das Gerät erneut mit dem vCenter registrieren.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Standardmäßiges Zertifikat für HTTPS-Zertifikate wiederherstellen**.
5. Klicken Sie im Dialogfeld „Standardmäßiges Zertifikat wiederherstellen" auf **Anwenden**.

Einrichten globaler Alarme

Mit der Alarmverwaltung können Sie globale Einstellungen, wie Alarme für alle vCenter-Instanzen gespeichert werden, festlegen.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung" in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **ALARMVERWALTUNG**. Klicken Sie auf **Bearbeiten**, um neue vCenter-Alarmeinstellungen festzulegen.
4. Geben Sie numerische Werte für die folgenden Elemente ein:
   - Maximale Anzahl an Alarmen
   - Anzahl an Tagen, über die Alarme beibehalten werden sollen
   - Timeout für duplizierte Alarme (Sekunden)
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Verwalten von Backups und Wiederherstellungen

Die Verwaltung von Backups und Wiederherstellungen erfolgt über die Administrator Console. Die Tasks auf dieser Seite umfassen:

- Konfigurieren von Backup und Wiederherstellung
- Planen von automatischen Backups
- Durchführen eines sofortigen Backups
- Wiederherstellen der Datenbank aus einem Backup

Konfigurieren von Backup und Wiederherstellung

Die Funktionen für das Backup und die Wiederherstellung sichern die Datenbank des OpenManage Integration for VMware vCenter an einem remoten Speicherort, von dem aus sie zu einem späteren Zeitpunkt wieder hergestellt werden kann. Profile, Vorlagen und Host-Informationen sind im Backup eingeschlossen. Wir empfehlen, dass Sie zum Schutz gegen Datenverlust automatische Backups planen. Nach diesem Verfahren müssen Sie einen Backup-Zeitplan konfigurieren.

 **ANMERKUNG:** NTP-Einstellungen werden nicht gesichert.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Bearbeiten**, um die aktuellen Einstellungen für Backup und Wiederherstellung zu bearbeiten.
5. Führen Sie auf der Seite **Einstellungen und Details** die folgenden Schritte aus:
   a. Geben Sie den Pfad zu den gesicherten Dateien in das Textfeld **Speicherort des Backups** ein.
   b. Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   d. Geben Sie das Verschlüsselungskennwort in das Textfeld **Kennwort für die Verschlüsselung von Backups** ein.

      Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
   e. Geben Sie das Verschlüsselungskennwort erneut in das Textfeld **Kennwort bestätigen** ein.
6. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.
7. Konfigurieren Sie den Backup-Zeitplan. Weitere Informationen finden Sie unter Planen von automatischen Backups.

Planen von automatischen Backups

Dies ist der zweite Teil der Konfiguration von Backup und Wiederherstellung. Ausführliche Informationen zum Konfigurieren des Backup-Speicherorts und des Berechtigungsnachweises finden Sie unter Konfigurieren von Backup und Wiederherstellung.
So konfigurieren Sie ein automatisches Backup:

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Bearbeiten Automatisch geplanter Backup**, um die Einstellungen für Backup und Wiederherstellung zu ändern. Das Feld wird aktiviert.
5. Klicken Sie auf **Aktiviert**, um Backups zu aktivieren.
6. Aktivieren Sie die Kontrollkästchen der Tage, an denen ein Backup durchgeführt werden soll .
7. Geben Sie die Zeit in dem Format HH:MM in das Textfeld **Uhrzeit für Backup (24 Stunden Uhrzeitformat, HH:mm)** ein.

   Das Feld **Nächster Backup** wird mit dem Datum und der Uhrzeit für den nächsten geplanten Backup ausgefüllt.
8. Klicken Sie auf **Anwenden**.

Durchführen eines sofortigen Backups

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Jetzt sichern**.
5. Aktivieren Sie im Dialogfeld **Jetzt sichern** das entsprechende Kontrollkästchen, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
6. Geben Sie einen **Speicherort für das Backup**, einen **Benutzernamen**, ein **Kennwort** und das **Verschlüsselungskennwort** ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
7. Klicken Sie auf **Sichern**.

Wiederherstellen der Datenbank aus einem Backup

ANMERKUNG: Bei einer Wiederherstellung wird das virtuelle Geräte nach Abschluss der Wiederherstellung neu gestartet wird.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**. Die aktuellen Einstellungen für das Backup und die Wiederherstellung werden angezeigt.
4. Klicken Sie auf **Jetzt wiederherstellen**.
5. Geben Sie einen **Dateispeicherort (CIFS/NFS-Format)** in das Dialogfeld „Jetzt wiederherstellen“ ein.
6. Geben Sie den **Benutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
7. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

   Das Gerät wird neu gebootet oder startet neu, nachdem Sie auf „Anwenden“ geklickt haben.

Grundlegendes zur vSphere Client-Konsole

Die **Konsole** befindet sich innerhalb des vSphere-Clients auf einer virtuellen Maschine. Die **Konsole** arbeitet Hand in Hand mit der Administrationskonsole. Die Konsole ermöglicht die Ausführung folgender Aufgaben:

- Konfiguration von Netzwerkeinstellungen
- Ändern des Kennworts des virtuellen Geräts
- Einstellen der lokalen Uhrzeit
- Neustart des virtuellen Geräts
- Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen
- Aktualisieren der Konsole
- Option Abmelden

Verwenden Sie die Pfeiltasten, um nach oben oder unten zu navigieren. Wenn Sie die gewünschte Option einmal ausgewählt haben, drücken Sie die **<EINGABETASTE>**. Wenn Sie auf den **Konsole**nbildschirm zugreifen, übernimmt der VMware vSphere-Client die Kontrolle Ihres Cursors. Um dieser Kontrolle zu entgehen, drücken Sie **<STRG> + <ALT>**.

Konfigurieren der Netzwerkeinstellungen

Die Netzwerkeinstellungen werden im vSphere-Client auf der Konsole eingerichtet.

1. Wählen Sie im vSphere-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
    - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Wählen Sie im Fenster **Konsole** die Option **Netzwerk konfigurieren** und drücken Sie die **<EINGABETASTE>**.
5. Geben Sie die gewünschten Netzwerkeinstellungen unter **Geräte bearbeiten** oder unter **DNS bearbeiten** ein und klicken Sie auf **Speichern und Beenden**. Klicken Sie auf **Beenden**, um die Änderungen zu verwerfen.

Ändern des Kennworts des virtuellen Geräts

Das Kennwort des virtuellen Geräts wird im vSphere Web-Client auf der Registerkarte „Konsole“ geändert.

1. Wählen Sie im vSphere Web-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
    - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Wählen Sie in der Konsole mit den Pfeiltasten die Option **Admin-Kennwort ändern** aus und drücken Sie die **<EINGABETASTE>**.
5. Geben Sie das **Aktuelle Admin-Kennwort** ein und drücken Sie die **<EINGABETASTE>**.

    Admin-Kennwörter müssen ein Sonderzeichen, eine Zahl, einen Großbuchstaben, einen Kleinbuchstaben und mindestens acht Buchstaben umfassen.
6. Geben Sie ein neues Kennwort unter **Neues Admin-Kennwort eingeben** ein und drücken Sie die **<EINGABETASTE>**.
7. Geben Sie das neue Kennwort erneut in das Textfeld **Admin-Kennwort bestätigen** ein und drücken Sie die **<EINGABETASTE>**.

Einstellen der lokalen Uhrzeit

So stellen Sie die lokale Uhrzeit ein:

1. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie im **vSphere-Client** die virtuelle OpenManage Integration for VMware vCenter-Maschine aus, und klicken Sie dann auf die Registerkarte **Konsole**
    - Wählen Sie **Zeitzone einstellen** und drücken Sie die **<EINGABETASTE>**.
2. Wählen Sie im Fenster **Zeitzonenauswahl** die gewünschte Zeitzone aus und klicken Sie auf **OK**. Um Änderungen zu verwerfen, klicken Sie auf **Abbrechen**. Die Zeitzone wird aktualisiert. Sie können nur die Zeitzone bearbeiten, aber nicht die aktuelle Uhrzeit oder das Datum

Neustarten des virtuellen Geräts

So starten Sie das virtuelle Gerät neu:

1. Wählen Sie im vSphere Web-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Verwenden Sie die Pfeiltasten zur Auswahl von **Dieses virtuelle Gerät neu starten** und drücken Sie die **<EINGABETASTE>**.
5. Die folgende Meldung wird angezeigt:

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
6. Drücken Sie **j**, um den Neustart fortzusetzen, oder drücken Sie **n**, um den Vorgang abzubrechen. Das Gerät wird neu gestartet.

Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen

So setzen Sie das virtuelle Gerät auf die werkseitigen Einstellungen zurück:

1. Wählen Sie im vSphere-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Verwenden Sie die Pfeiltasten, um **Dieses virtuelle Gerät auf werkseitige Einstellungen zurücksetzen** auszuwählen, und drücken Sie auf die **<EINGABETASTE>**.
5. Die folgende Meldung wird angezeigt:

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```
6. Geben Sie **y** zum Zurücksetzen oder **n** zum Abbrechen ein. Das Gerät wird auf die ursprünglichen werksseitigen Standardeinstellungen zurückgesetzt und alle anderen Einstellungen und gespeicherten Daten gehen dabei verloren.

    **ANMERKUNG:** Wenn das virtuelle Gerät auf die werkseitigen Einstellungen zurückgesetzt wird, werden alle Aktualisierungen an der Netzwerkkonfiguration beibehalten; diese Einstellungen werden nicht zurückgesetzt.

Aktualisieren der Konsolenansicht

Wählen Sie **Aktualisieren**, um die Konsolenansicht zu aktualisieren, und drücken Sie die **<EINGABETASTE>**.

Schreibgeschützte Benutzerrolle

Es gibt eine Benutzerrolle ohne Rechte mit der Bezeichnung „Nur-Lesen“ mit Shell-Zugriff für Diagnosezwecke. Der Nur-Lesen-Benutzer verfügt über eingeschränkte Rechte zum Ausführen der eingehängten Geräte. Das Kennwort des Nur-Lesen-Benutzers entspricht dem des Administrators.

Migrationspfad zur Migration von 1.6/1.7 auf 2.3

Es gibt keine Unterstützung für die RPM-Aktualisierung von Version 1.7. oder früher auf diese Version. Sie können mithilfe des Backup- und Wiederherstellungspfads eine Aktualisierung von einer älteren Version (1.6 oder 1.7) auf Version 2.3 durchführen. Der Migrationspfad wird ebenfalls nur ausgehend von Version 1.6 oder 1.7 unterstützt. Wenn Sie eine Version vor Version 1.6 ausführen, müssen Sie eine Erweiterung Ihres Geräts auf die unterstützte Version durchführen, bevor Sie mit der Migration auf OpenManage Integration for VMware vCenter Version 2.3 beginnen.

Führen Sie die folgenden Schritte durch, um von einer älteren Version auf OpenManage Integration for VMware vCenter Version 2.3 zu migrieren:

1. Erstellen Sie eine Sicherungskopie der Datenbank der älteren Versionen. Weitere Informationen finden Sie in den Abschnitten **Managing Backup and Restore** (Verwalten von Sicherung und Wiederherstellung) in diesem Handbuch.
2. Fahren Sie die älteren Geräte des vCenters herunter.

   ANMERKUNG: Heben Sie nicht die Registrierung des vCenter-Plugins auf. Das Aufheben der vCenter-Plugin-Registrierung entfernt alle auf dem Plugin durch vCenter registrierten Alarme und alle benutzerdefinierten Vorgänge, wie Maßnahmen auf dem vCenter. Weitere Informationen finden Sie im Abschnitt **Wiederherstellung nach dem Aufheben der Registrierung des älteren Plugins nach einem Backup** in diesem Handbuch, sollten Sie das Aufheben der Registrierung des Plugins nach einem Backup bereits vorgenommen haben.
3. Stellen Sie die neue OpenManage Integration Version 2.3 OVF bereit. Weitere Informationen zur Bereitstellung des OVFs finden Sie im Abschnitt **Bereitstellen des OpenManage Integration for VMware vCenter OVF unter Verwendung des vSphere Clients** in diesem Handbuch.
4. Starten Sie das OpenManage Integration Version 2.3-Gerät.
5. Stellen Sie das Netzwerk, die Zeitzone usw. auf dem Gerät ein. Es wird empfohlen, dass das neue OpenManage Integration Version 2.3-Gerät dieselbe IP-Adresse, wie das alte Gerät hat. Weitere Informationen zum Einstellen der Netzwerkdetails finden Sie im Abschnitt **Registrierung des OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei** in diesem Handbuch.
6. Wiederherstellen der Datenbank auf dem neuen Gerät. Weitere Informationen finden Sie im Abschnitt **Wiederherstellen der Datenbank mithilfe eines Backups** in diesem Handbuch.
7. Laden Sie die neue Lizenzdatei hoch. Weitere Informationen finden Sie im Abschnitt **Registrieren von OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei** im **OpenManage Integration Version 2.3 Quick Install Guide** (Schnellinstallationsanleitung).
8. Überprüfen des Geräts. Weitere Informationen zum Sicherstellen, dass die Datenbankmigration erfolgreich war, finden Sie im Abschnitt **Überprüfung der Installation** in diesem Handbuch.
9. Führen Sie die Bestandsaufnahme auf allen registrierten vCentern aus.

ANMERKUNG:

Es wird empfohlen, dass Sie die Bestandsaufnahme auf allen durch das Plugin verwalteten Hosts nach der Aktualisierung durchführen. Weitere Informationen zum Ausführen der Bestandsaufnahme nach Bedarf finden Sie im Abschnitt **Ausführen von Bestandsaufnahme-Jobs**.

Sollte die IP-Adresse des neuen OpenManage Integration Version 2.3-Geräts von der des alten Geräts abweichen, muss das Trap-Ziel der SNMP-Traps so konfiguriert werden, dass es auf das neue Gerät verweist. Bei Servern ab der 12. Generation wird das Problem durch Ausführen der Bestandsaufnahme auf diesen Hosts behoben. Für alle Hosts der 11. oder einer noch älteren Generation, die früher konform waren, wird die IP-Adresse als nicht konform angezeigt und die Konfiguration von OMSA ist erforderlich. Weitere Informationen zum Reparieren der Host-Übereinstimmung finden Sie im Abschnitt **Ausführen des Assistenten zum Reparieren von nicht konformen vSphere-Hosts** in diesem Handbuch.

7

Einstellungen

Die Registerkarte „Einstellungen“ wird für folgendes verwendet:

- Anzeigen der Garantieablaufbenachrichtigungseinstellungen
- Garantieablaufbenachrichtigung anzeigen
- Einrichten des Firmware-Aktualisierungs-Repositorys
- Anzeigen der Alarm- und Ereigniseinstellungen
- Konfigurieren und Verwalten von Ereignissen und Alarmen
- Anzeigen und Konfigurieren der Datenabrufszeitpläne für Bestandsaufnahme und Garantie

Bearbeiten des OMSA-Links

Dieses Verfahren geht davon aus, dass Sie bereits einen OMSA Web Server installiert haben und dass Sie diesen Link unter Verwendung des Konfigurationsassistenten zuvor bereits konfiguriert haben. Lesen Sie das *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator Installationshandbuch), um etwas über die Version des in Verwendung befindlichen OMSAs zu erfahren und Anweisungen zur Installation und Konfiguration des Web Servers zu erhalten.
Wenn Sie nicht bereits während der Ausführung des Konfigurationsassistenten einen Link bereitgestellt haben, dann können Sie diesen Link auf der Registerkarte OpenManage Integration for VMware vCenter **Einstellungen** → **verwalten** bearbeiten.



ANMERKUNG: OMSA wird nur auf Dell PowerEdge-Servern der 11. Generation oder älter benötigt. Der Web Client Initial Configuration-Assistent verfügt nicht über eine Option den OMSA-Link bereitzustellen. Der OMSA-Link ist nur für .net-Client gültig.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf dem Register **Verwalten** → **Einstellungen** unter vCenter-Einstellungen und rechts von der OMSA Web Server-URL auf **Bearbeiten**.
2. Geben Sie im OMSA Web Server-URL Dialogfeld die **URL** ein.

   Es muss die volle URL einschließlich des HTTPS enthalten sein.
3. Markieren Sie das Kontrollkästchen **Diese Einstellungen auf alle vCenters anwenden**, um die OMSA-URL auf alle vCenters anzuwenden. Falls Sie dieses Kontrollkästchen nicht markieren, wird die OMSA-URL nur auf ein vCenter angewandt.
4. Überprüfen Sie, dass der Link funktioniert, indem Sie zum Host-Zusammenfassungsregister für diesen Host navigieren. Überprüfen Sie, dass der OMSA-Konsolenlink in den Dell Hostinformationen funktioniert.

Verwendung von OMSA mit Servern der 11. Generation verstehen

Auf Servern vor der 12. Dell PowerEdge-Generation muss OMSA installiert werden, damit Dell OpenManage Integration for VMware vCenter ordnungsgemäß funktioniert. OMSA wird auf Dell PowerEdge-Hosts der 11. Generation automatisch im Rahmen der Bereitstellung installiert, Sie können jedoch immer noch eine manuelle Installation durchführen, falls Sie dies wünschen.

Wählen Sie für die Konfiguration von OMSA auf Dell PowerEdge-Hosts der 11. Generation unter den folgenden Optionen aus:

- Bereitstellen eines OMSA-Agenten auf einem ESXi-System
- Bereitstellen eines OMSA-Agenten auf einem ESX-System
- Einrichten eines OMSA-Trap-Ziels

 ANMERKUNG: Abgesehen von den oben genannten Optionen können Sie den .NET-Client verwenden und die Option „Host-Konformität“ ausführen. Auf diese Weise können Sie den OMSA-Agenten installieren und konfigurieren.

Bereitstellen eines OMSA-Agenten auf einem ESX-System

Installieren Sie die OMSA-Datei tar.gz auf einem ESX-System, um eine Bestandsliste und Alarminformationen der Systeme zu erstellen.

 ANMERKUNG: OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

So stellen Sie die OMSA-Agent-Datei tar.gz auf einem ESX-System mit der erforderlichen Remote-Aktivierungseinstellung (-c) bereit:

1. Führen Sie das OMSA-Agent-Installationsskript aus:
   `srvadmin-install.sh -x -c`
2. Starten Sie die OMSA-Dienste:
   `srvadmin-services.sh start`
3. Wenn der OMSA-Agent bereits installiert wurde, stellen Sie sicher, dass die Remote-Aktivierungseinstellung (-c) konfiguriert ist, anderenfalls kann die Installation des OpenManage Integration for VMware vCenter nicht erfolgreich abgeschlossen werden. Installieren Sie sie mit der Option -c erneut und starten Sie den Dienst neu:
   `srvadmin-install.sh -c srvadmin-services.sh restart`

Bereitstellen eines OMSA-Agenten auf einem ESXi-System

Installieren Sie den OMSA VIB auf einem ESXi-System, um eine Bestandsliste und Alarminformationen von den Systemen zu erstellen.

 ANMERKUNG: OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. Falls noch nicht geschehen, installieren Sie das vSphere-Befehlszeilentool (vSphere CLI) von **http://www.vmware.com**.
2. Geben Sie folgenden Befehl ein:
   `Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>`

    ANMERKUNG: Die Installation von OMSA kann einige Minuten dauern. Dieser Befehl erfordert einen Neustart des Hosts nach Abschluss der Installation.

Einrichten eines OMSA-Trap-Ziels

Diese Aufgabe ist nur für Hostsysteme erforderlich, die OMSA anstelle von iDRAC6 zum Erzeugen von Ereignissen verwenden. Für iDRAC6 ist keine zusätzliche Konfiguration erforderlich.

ANMERKUNG: OMSA ist nur auf Dell-Servern erforderlich, die älter als die 12. Dell PowerEdge-Server-Generation sind.

1. Verwenden Sie entweder den Link zur OMSA-Benutzeroberfläche in der Registerkarte OpenManage Integration for VMware vCenter **Einstellungen** → **verwalten**, oder navigieren Sie mittels eines Webbrowsers zum OSMA-Agenten (**https://<HostIP>:1311/**).
2. Melden Sie sich an und wählen Sie die Registerkarte **Alarmverwaltung**.
3. Wählen Sie **Alarm-Aktionen** und stellen Sie sicher, dass die Option **Broadcast-Nachricht** für alle zu überwachenden Ereignisse gesetzt ist, so dass die Ereignisse gesendet werden.
4. Wählen Sie oben auf der Registerkarte die Option **Plattformereignisse** aus.
5. Klicken Sie auf die graue Schaltfläche **Ziele konfigurieren** und dann auf den Link **Ziel**.
6. Aktivieren Sie das Kontrollkästchen **Ziel aktivieren**.
7. Geben Sie die OpenManage Integration for VMware vCenter Geräte-IP-Adresse in das Feld **Ziel-IP-Adresse** ein.
8. Klicken Sie auf **Änderungen anwenden**.
9. Wiederholen Sie die Schritte 1 bis 8, um weitere Ereignisse zu konfigurieren.

Anzeigen der Garantieablaufbenachrichtigungseinstellungen

1. Klicken Sie im OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen**unter Geräteeinstellungen auf **Garantieablaufbenachrichtigung**.
2. Unter Garantieablaufbenachrichtigung können Sie folgendes anzeigen lassen:
   - Aktivierungs- oder Deaktivierungsstatus der Einstellung.
   - Einstellung der Anzahl der Tage bis zur ersten Warnung.
   - Einstellung der Anzahl der Tage bis zur krtischen Warnung.
3. Lesen Sie für die Konfiguration der Garantieablaufbenachrichtigung Garantieablaufbenachrichtigungseinstellungen konfigurieren.

Garantieablaufbenachrichtigung anzeigen

Sie können Garantieablaufschwellenwerte konfigurieren, die Sie über den Ablauf der Garantie informieren.

1. Klicken Sie im OpenManage Integration for VMware vCenter auf dem Register **Verwalten** → **Einstellungen**unter Geräteeinstellungen auf der rechten Seite von **Garantieablaufbenachrichtigung** auf das Symbol **Bearbeiten**.
2. Verfahren Sie im Dialogfeld „Garantieablaufinformationen“ wie folgt:
   a. Falls Sie diese Einstellung aktivieren möchten, markieren Sie das Kontrollkästchen **Garantieablaufbenachrichtigung für Hosts aktivieren**.

      Das Wählen des Kontrollkästchens aktiviert die Garantieablaufbenachrichtigung.
   b. Verfahren Sie unter „Mindesttageschwellenwertalarm“ wie folgt:
      1. Wählen Sie in der Drop-Down-Liste „Warnung“ den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf der Garantie gewarnt werden wollen.
      2. Wählen Sie in der Drop-Down-Liste „Kritisch“ den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf der Garantie gewarnt werden wollen.
3. Klicken Sie auf **Anwenden**.

Konfigurieren von Ereignissen und Alarmen

Detaillierte Informationen über Ereignisse und Alarme finden Sie unter Verstehen von Alarmen und Ereignissen. Konfigurieren Sie Ereignisse und Alarme auf der Registerkarte OpenManage Integration for VMware vCenter

Verwaltungs → einstellungen. Unter vCenter-Einstellungen erweitern Sie die Überschrift „Ereignisse und Alarme“, um die aktuellen vCenter-Alarme für Dell-Hosts (aktiviert oder deaktiviert) anzuzeigen, oder für alle und die Ereignisanzeigeebene.

ANMERKUNG: Bei Hosts vor der Version der Dell PowerEdge-Server der 12. Generation erfordert diese Funktion, dass das virtuelle Gerät als ein Trap-Ziel in OMSA konfiguriert ist, um Host-Ereignisse im vCenter anzuzeigen. Weitere Informationen zu OMSA finden Sie unter Einrichten eines OMSA Trap-Zieles.

ANMERKUNG: Um Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

1. Auf der Registerkarte OpenManage Integration for VMware vCenter **Verwalten → Einstellungen** neben den vCenter-Einstellungen verwenden Sie die Dropdown-Liste zur Auswahl des vCenter-Servers oder aller vCenter-Server, die in dieser Einstellung eingeschlossen sind.

   Falls Sie „Alle registrierten Server“ ausgewählt haben, werden die Optionen evtl. leer angezeigt. Dies ermöglicht Ihnen die Konfiguration der Einstellungen für alle registrierten vCenters auf einmal. Falls die vCenters dieselben Einstellungen haben, werden diese angezeigt.
2. Klicken Sie auf der rechten Seite von „Ereignisse und Alarme“ auf das Symbol **Bearbeiten**.
3. Aktivieren Sie das Kontrollkästchen **Alarme für alle Dell-Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Dell-Hosts mit aktivierten Alarmen reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus übergehen, und Sie können den Alarm nach Bedarf ändern.
4. Klicken Sie auf **Standard Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.
5. Wählen Sie eine der folgenden Optionen unter **Übermittlungsebene für das Ereignis**:

   - Keine Ereignisse anzeigen

     Diese Option blockiert Hardware-Ereignisse.
   - Alle Ereignisse anzeigen

     Diese Option veröffentlicht alle Hardware-Ereignisse.
   - Nur kritische Ereignisse und Warnungsereignisse anzeigen

     Diese Option veröffentlicht nur kritische Hardwareereignisse oder Ereignisse mit Warnungsstufe.
   - Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen.

     Diese Option veröffentlicht nur virtualisierungsbezogene kritische Ereignisse und Warnungsereignisse. Dies ist die standardmäßige Einstellung der Veröffentlichungsstufe.
6. Falls Sie diese Einstellungen auf alle vCenters anwenden möchten, markieren Sie das Kontrollkästchen **Diese Einstellungen auf alle vCenters anwenden**.

   ANMERKUNG: Die Auswahl dieser Option überschreibt die vorhandenen Einstellungen für alle vCenters.

   Diese Option ist ausgeblendet, wenn Sie bereits 'Alle registrierten vCenter' aus der Dropdown-Liste der Einstellungsseite ausgewählt haben.
7. Klicken Sie zum Speichern auf **Anwenden**.

Anzeigen der Alarm- und Ereigniseinstellungen

Sobald Alarme und Ereignisse konfiguriert wurden, können Sie anzeigen lassen, ob die vCenter-Alarme für Hosts aktiviert sind und welche Ereignisveröffentlichungsstufe auf der Registerkarte „Einstellungen“ ausgewählt wurde.

1. Erweitern Sie im Register OpenManage Integration for VMware vCenter**Verwalten → Einstellungen** unter „vCenter-Einstellungen“ „Ereignisse und Alarme“.
2. Unter „Ereignisse und Alarme“ können Sie folgendes anzeigen lassen:

- vCenter-Alarme für Dell Hosts: zeigt entweder „Aktiviert“ oder „Deaktiviert“ an.
- Ereignis-Veröffentlichungsstufe

  Lesen Sie für die anzeigbaren Ereignis-Veröffentlichungsstufen unter Ereignisse und Alarme verstehen nach.

3. Lesen Sie zum Konfigurieren von Alarmen und Ereignissen Konfigurieren von Alarmen und Ereignissen

Anzeigen von Ereignissen

Konfigurieren Sie Ereignisse, bevor Sie diese in der Registerkarte „Ereignisse“ anzeigen lassen können. Siehe Konfigurieren von Ereignissen und Alarmen.
Lassen Sie die Ereignisse für einen Host, Cluster oder Datacenter auf der Registerkarte „Ereignisse“ anzeigen.

1. Klicken Sie im Navigator des OpenManage Integration for VMware vCenter auf **Hosts**, **Datacenter** oder **Cluster**.
2. Wählen Sie auf der Registerkarte „Objekte“ einen spezifischen Host, ein Datacenter oder einen Cluster aus, für den Sie Ereignisse anzeigen lassen wollen.
3. Klicken Sie auf der Registerkarte „Überwachen“ auf **Ereignisse**.
4. Wählen Sie ein spezifisches Ereignis aus, um weitere Ereignisdetails anzeigen zu lassen.

Allgemeines zu Firmware-Aktualisierungen

Der Standort, auf dem Server Firmware-Aktualisierungen erhalten, ist eine globale Einstellung, die im OpenManage Integration for VMware vCenter im Register „Einstellungen“ verfügbar ist.

Die Einstellungen für das Firmware-Repository enthalten den Speicherort des Firmware-Katalogs, der zum Aktualisieren von bereitgestellten Servern verwendet wird. Es gibt zwei Arten von Speicherorten:

Dell (ftp.dell.com)	Verwendet das Repository zur Firmware-Aktualisierung von Dell (**ftp.dell.com**). OpenManage Integration for VMware vCenterr lädt die ausgewählten Firmware-Aktualisierungen von Dell herunter.
Freigegebene Netzwerkordner	Erstellt mit Dell Repository Manager™. Diese lokalen Repositorien befinden sich auf der CIFS- oder der NFS-Dateifreigabe.



ANMERKUNG: Nachdem ein Repository erstellt wurde, speichern Sie es an einem Speicherort, auf den registrierte Hosts zugreifen können. Die Kennwörter für Repositorien dürfen nicht mehr als 31 Zeichen umfassen. Folgende Zeichen dürfen dabei nicht verwendet werden: @, &, %, ', ", ,(Komma), < >

Der Assistent zur Aktualisierung der Firmware prüft stets die erforderlichen Mindest-Firmware-Versionen für iDRAC, BIOS und den Lifecycle Controller und versucht, diese auf die erforderlichen Mindestversionen zu aktualisieren. Wenn die iDRAC-, Lifecycle- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Assistent zur Aktualisierung der Firmware alle Firmware-Aktualisierungen, einschließlich iDRAC, Lifecycle Controller, RAID, NIC/LOM, Netzteile, BIOS usw.



ANMERKUNG: Bei Servern der 9. und 10. Generation können die BIOS/BMC/DRAC-Firmware-Versionen nur auf der „Cluster View“-Ebene in vCenter oder auf der Seite „Übersicht“ in der individuellen Hostansicht angezeigt werden. Die Informationen zur Firmware-Version sind in der individuellen Hostansicht unter „Firmware“ nicht aktiv und remote Firmware-Aktualisierungen stehen nicht zur Verfügung.

Firmware-Versionen nach dem 14. Oktober 2010

Bei Firmware, die am oder nach dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware ausgeführt.

Firmware-Versionen neuer als 29. Juli 2009 und vor dem 14. Okober 2010

Wenn Ihre Firmware am oder nach dem 29. Juli 2009 und vor dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware nicht angezeigt, stattdessen erhalten Sie ein ISO-Paket zur Aktualisierung Ihrer Firmware. Auch nach dieser Aktualisierung verfügen Sie eventuell noch nicht über die aktuellste Firmware. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Firmware-Versionen vor 29. Juli 2009

Wenn Ihre Firmware älter als 29. Juli 2009 ist, müssen Sie die ISO-Datei herunterladen und ausführen, um Ihre Maschinen zu aktualisieren. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Weitere Informationen:

- Einrichten des Firmware-Repositorys

Einrichten des Firmware-Aktualisierungs-Repositorys

Sie können das Repository für die Firmwareaktualisierung auf der Registerkarte der Einstellungen für OpenManage Integration for VMware vCenter einrichten.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf dem Register **Verwalten** → **Einstellungen** unter Geräteeinstellungen und auf der rechten Seite des Repository für die Firmwareaktualisierung auf das Symbol **Bearbeiten**.
2. Wählen Sie im Dialogfeld Firmware-Aktualisierungs-Repository eine der folgenden Optionen aus:
   - Dell Online

     Standard-Firmware-Repository (ftp.dell.com) mit einem Arbeitsordner. Die OpenManage Integration for VMware vCenter lädt ausgewählte Firmwareaktualisierungen herunter und speichert sie im Arbeitsordner, und dann müssen Sie den Firmwareassistenten ausführen, um die Firmware zu aktualisieren.
   - Freigegebene Netzwerkordner

     Diese werden mit der Anwendung Dell Repository Manager erstellt. Sie finden diese lokalen Repositorys auf windowsbasierten Dateifreigaben. Verwenden Sie den Live-Link, um zum Dell Repository Manager zu gehen.
3. Wenn Sie **Freigegebenen Netzwerkordner** ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie den **Speicherort der Katalogdatei** in der folgenden Syntax ein:
      - NFS-Freigabe für xml-Datei: host:/share/filename.xml
      - NFS-Freigabe für gz-Datei: host: /share/filename.gz
      - CIFS-Freigabe für xml-Datei: \\host\share/filename.xml
      - CIFS-Freigabe für gz-Datei: \\host\share/filename.gz

   b. Falls das Herunterladen der Dateien im ausgewählten Repository-Pfad läuft, der auf dem Bildschirm **Aktualisierungsquelle auswählen** angezeigt wird, wird eine Fehlermeldung angezeigt, die besagt, dass der Download läuft.
4. Wenn das Herunterladen der Datei abgeschlossen ist, klicken Sie auf **Anwenden**.

Ausführen des Firmwareaktualisierungsassistenten für einen einzelnen Host

Diese Funktionalität steht nur für die 11., 12. und 13. Generation von Dell-Servern zur Verfügung, die entweder eine iDRAC Express- oder eine Enterprise-Karte haben. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversion automatisch mit dem Firmware-Update-Assistenten aktualisieren.



ANMERKUNG: Ändern Sie zum Schutz gegen Fehler durch Zeitüberschreitung des Browsers die Standardzeit auf 30 Sekunden. Weitere Informationen zum Ändern der Standardzeitüberschreitungseinstellungen finden Sie unter „Warum wird eine Fehlermeldung nachdem ich auf den Firmware-Aktualisierungslink geklickt habe, angezeigt?" im Abschnitt „Fehlerbehebung" im *Benutzerhandbuch*.

ANMERKUNG: Rechtsklicken Sie auf **Host** > **Alle OpenManage Integrationsmaßnahmen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten. Oder klicken Sie auf **Host** > **Maßnahmen** > **Alle OpenManage Integrationsmaßnahmen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten. Oder klicken Sie auf **Host** > **Zusammenfassung** > **Dell Hostinformationen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten.

So führen Sie den Firmware-Update-Assistenten aus:

1. Klicken Sie im **vSphere Web-Client** auf **Hosts**. Die Liste verfügbarer Hosts wird angezeigt.
2. Wählen Sie einen Host aus der angezeigten Liste aus.
3. Klicken Sie im Hauptmenü auf **Überwachen** und wählen Sie dann die Registerkarte **Dell-Hostinformationen**. Die Bestandsaufnahmedaten der Dell-Hosts werden angezeigt.
4. Klicken Sie auf **Firmware**, und die verfügbaren Firmwareversionen mit den Details werden angezeigt.
5. Klicken Sie auf **Firmwareassistent ausführen**. Der Bildschirm **Firmwareaktualisierung** wird angezeigt.
6. Klicken Sie auf **Weiter**. Daraufhin wird der Bildschirm **Aktualisierungsquelle auswählen** mit dem Firmware-Aktualisierungsbündel für den angegebenen Host angezeigt. Wählen Sie auf dem Bildschirm das Firmware-Aktualisierungsbündel aus der Dropdown-Liste **Ein Aktualisierungsbündel auswählen** aus.
7. Klicken Sie auf **Weiter**. Der Bildschirm **Komponenten auswählen** wird angezeigt. Dieser listet die Firmwaredetails für die Komponenten auf.
8. Wählen Sie die gewünschten Firmwareaktualisierungen aus und klicken Sie auf **Weiter**. Komponenten, die zurückgestuft wurden, bereits aktuell sind oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Falls Sie das Kontrollkästchen **Zurückstufung der Firmware gestatten** markieren, wählen Sie die Optionen aus, die als Zurückstufung aufgeführt sind. Die Auswahl dieser Option ist nur fortgeschrittenen Benutzern empfohlen, die die Folgen einer Zurückstufung der Firmware verstehen.
9. Klicken Sie auf **Weiter.** Der Bildschirm **Firmwareaktualisierung planen** wird angezeigt.

   - Geben Sie den Jobnamen im Feld **Jobname der Firmwareaktualisierung** und die Beschreibung im Feld **Beschreibung der Firmwareaktualisierung** ein. Diese Feldeingabe ist optional.
   - Wählen Sie **Jetzt aktualisieren** zum sofortigen Start der Firmwareaktualisierung.
   - **Aktualisierung planen**, wählen Sie diese Schaltfläche aus, um den Firmwareaktualisierungsjob später auszuführen, und klicken Sie auf **Weiter**. Sie können den Firmwareaktualisierungsjob für 30 Minuten nach der aktuellen Uhrzeit planen.
   - Wählen Sie im Kontrollkästchen Kalender den Monat und Tag aus.
   - Geben Sie im Textfeld „Zeit“ die Uhrzeit im Format HH:MM ein, und klicken Sie dann auf „Weiter“. Die Uhrzeit entspricht der lokalen Ortszeit, wo Ihr Client sich physisch befindet. Ungültige Zeitwerte könnten zu einer blockierten Aktualisierung führen.
   - **Wenden Sie die Aktualisierungen beim nächsten Neustart an.**

     Um eine Dienstunterbrechung zu vermeiden, wird empfohlen, dass der Host vor dem Neustart in den Wartungsmodus übergeht.
   - **Aktualisierungen anwenden und den Neustart erzwingen, ohne in den Wartungsmodus überzugehen.**

     Die Aktualisierung wird angewandt, und ein Neustart wird ausgeführt, auch wenn der Host nicht im Wartungsmodus ist. Diese Methode ist nicht empfehlenswert.
10. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Details über alle Komponenten nach der Firmwareaktualisierung bereit.
11. Klicken Sie auf **Fertigstellen**.
12. Um zu überprüfen, dass die Aktualisierung erfolgreich verlaufen ist, wählen Sie im Register **Überwachen Job-Warteschlange** → **Firmwareaktualisierungen** und überprüfen Sie die Seite **OpenManage Integration-Übersicht**, um die neuen Versionen zu sehen.

Ausführen des Firmwareaktualisierungsassistenten für einen Cluster

Diese Funktion steht nur für Dell-Server der 11., 12. und 13. Generation zur Verfügung, die eine iDRAC Express- oder eine Enterprise-Karte haben. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversionen automatisch mit dem Firmwareaktualisierungsassistenten aktualisieren. Dieser Assistent aktualisiert nur Hosts, die Teil eines Verbindungsprofils sind und in Bezug auf Firmware, CSIOR-Status, Hypervisor und OMSA-Status (nur Server der 11. Generation) konform sind. Wählen Sie einen Cluster, der in der Clusteransicht aufgelistet ist, und verwenden Sie den Firmwareaktualisierungsassistenten. Es dauert normalerweise 30 bis 60 Minuten, um die Firmwarekomponenten aller Cluster zu aktualisieren. Aktivieren Sie DRS auf einem Cluster, damit virtuelle Maschinen migriert werden können, wenn ein Host den Wartungsmodus während der Firmwareaktualisierung betritt/verlässt. Sie können nur einen Firmwareaktualisierungs-Task auf einmal planen oder ausführen.

Verwenden Sie zum Export aus dem Assistenten die CSV-Taste. Die Suche steht für das Lokalisieren eines bestimmten Clusters, Datenzetrums, Host oder jeden Themenpunkt der Datentabelle außer für „Datum der Anwendung" zur Verfügung.

 **ANMERKUNG:** Aktualisieren Sie die Firmware immer zusammen als Teil des Repository-Pakets: BIOS, iDRAC und Lifecycle Controller.

 **ANMERKUNG:** Informationen über das Ändern der standardmäßigen Zeitüberschreitungseinstellung finden Sie im Abschnitt 'Fehlerbehebung' im *Benutzerhandbuch*.

Sie können den Status der Firmware-Aktualisierungs-Jobs auf der Seite „Job-Warteschlange" anzeigen und verwalten. Siehe Anzeige von Firmware-Aktualisierungen für Cluster und Datenzentren.

1. Klicken Sie auf das Symbol **OpenManage Integration,** dann auf **Cluster,** angezeigt im linken Bereich. Die Liste von Clustern wird angezeigt.
2. Klicken Sie auf einen Cluster in der angezeigten Liste. Das Hauptmenü wird mit verschiedenen Optionen angezeigt.
3. Klicken Sie auf **Überwachen** -->**Dell Clusterinformationen** -->**Firmware**. Der Bildschirm **Firmwareassistent ausführen** wird angezeigt.
4. Klicken Sie auf den Link **Firmwareassistent ausführen**. Die Seite **Willkommen** wird angezeigt.
5. Klicken Sie auf **Weiter**. Der Bildschirm **Aktualisierungsquelle auswählen** wird angezeigt; hier können Sie die Bündel auswählen. Der Repository-Standort wird auch angezeigt.
6. Wählen Sie den Host aus der angezeigten Liste im Bereich **Bündel auswählen** aus. Sie sollten mindestens ein Bündel für die Firmwareaktualisierung auswählen. Neben jedem Host gibt es eine Dropdown-Liste neben dem Hostnamen, aus der Sie das erforderliche Bündel auswählen können.
7. Klicken Sie auf **Weiter**. Der Bildschirm **Komponenten auswählen** wird angezeigt. Dieser Bildschirm enthält die Details von Komponenten, wie u. a. Modellname, Hostname, Service-Tag-Nummer, Komponente usw. für den ausgewählten Host.
8. Wählen Sie mindestens eine Komponente aus der Liste aus, und klicken Sie zum Fortfahren auf **Weiter**. Sie können den Inhalt des Komponentendatengitters mit dem Feld **Filtern** filtern oder Spalten innerhalb des Komponentendatengitters verschieben. Falls Sie das Kontrollkästchen **Firmwareherabstufung zulassen** markieren, wird die vorhandene Firmwareversion auf die vorherige verfügbare Version zurückgestuft.
9. Klicken Sie auf **Weiter**, und der Bildschirm **Firmwareaktualisierung planen** wird angezeigt.
   a. Geben Sie den Namen des Firmwareaktualisierungs-Jobs im Feld **Firmwareaktualisierungs-Jobname** ein. Dieser Wert ist obligatorisch.
   b. Geben Sie die Beschreibung der Firmwareaktualisierung im Feld **Firmwareaktualisierungsbeschreibung** ein. Dieser Wert ist optional.
10. Wählen Sie eine der folgenden Optionen aus.
    a. **Jetzt aktualisieren**, wählen Sie diese Schaltfläche aus, um den Firmwareaktualisierungsjob jetzt auszuführen, und klicken Sie auf **Weiter**.
    b. **Aktualisierung planen**: Wählen Sie diese Schaltfläche aus, um den Firmware-Aktualisierungsjob später auszuführen, und klicken Sie auf **Weiter**. Sie können den Firmware-Aktualisierungsjob für 30 Minuten nach der aktuellen Uhrzeit planen.

c. Wählen Sie im Kontrollkästchen **Kalender** den Monat und Tag aus.
d. Geben Sie im Textfeld **Zeit** die Uhrzeit im Format HH:MM ein, und klicken Sie dann auf **Weiter**. Die Uhrzeit ist die Ortszeit, wo Ihr Client sich befindet. Ungültige Zeitwerte führen zu einer blockierten Aktualisierung.

11. Der Bildschirm **Zusammenfassung** wird mit allen Firmwareaktualisierungsdetails angezeigt.
12. Klicken Sie auf **Fertig stellen,** und die Meldung **Der Firmwareaktualisierungsjob wurde erstellt** wird für die erfolgreiche Firmwareaktualisierung angezeigt.

Anzeige des Firmware-Aktualisierungs-Status für Cluster und Datenzentren

Damit Informationen auf dieser Seite angezeigt werden, führen Sie eine Firmwareaktualisierung aus oder planen Sie eine für einen Cluster oder Host.
Auf dieser Seite können Sie Firmware-Aktualisierungs-Jobs aktualisieren, säubern oder abbrechen.

1. Wählen Sie von OpenManage Integration **Überwachen** → **Job-Warteschlange** → **Firmwareaktualisierungen**.
2. Zum Anzeigen der aktuellsten Informationen klicken Sie auf **Aktualisieren**.
3. Anzeige des Status in der Datentabelle. Dieses Raster enthält die folgenden Informationen über Firmware-Aktualisierungs-Jobs:

   - Status
   - Geplante Zeit
   - Name
   - Beschreibung
   - vCenter
   - Erfassungsgröße

     Die Erfassungsgröße ist die Anzahl der Server auf diesem Firmware-Bestandsaufnahme-Job.
   - Fortschrittszusammenfassung

     Die Fortschrittszusammenfassung listet die Fortschrittsdetails dieser Firmware-Aktualisierung auf.
4. Um mehr Details über einen bestimmten Job im Datengitter für einen bestimmten Job anzuzeigen, klicken Sie auf ein Element des Masterdatengitters. Die Details werden im Detaildatengitter angezeigt.

   Hier finden Sie die folgenden Details:

   - Host-Name
   - Status
   - Startzeit
   - Endzeit
5. Wenn Sie eine geplante Firmware-Aktualisierung die nicht ausgeführt wird, abbrechen wollen, klicken Sie auf **Abbrechen**.
6. Falls Sie einen geplanten Job ändern möchten, klicken Sie auf **Ändern**.
7. Wenn Sie die geplanten Firmware-Aktualisierungen säubern möchten, klicken Sie auf **Job-Warteschlange säubern**.

   Sie können nur Jobs säubern, die erfolgreich abgeschlossen oder fehlgeschlagen oder aber abgebrochen sind.
8. Wählen Sie **Älter als Datum und Job-Status** aus und klicken Sie auf **Anwenden**. Die ausgewählten Jobs werden aus der Warteschlange entfernt.

Verstehen von Ereignissen und Warnmeldungen für Hosts

Sie können Ereignisse und Alarmeinstellungen von OpenManage Integration for VMware vCenter aus innerhalb der Registerkarte **Verwalten** → **Einstellungen**bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen,

Alarme für Dell Hosts aktivieren oder Standardalarme wiederherstellen. Sie können Ereignisse oder Alarme für einzelne vCenter oder alle registrierten vCenter gleichzeitig konfigurieren.

Es gibt vier Ereignis-Veröffentlichungsstufen.

Tabelle 2. Beschreibung der Ereignis-Veröffentlichungsstufen

Ereignis	Beschreibung
Keine Ereignisse anzeigen	OpenManage Integration for VMware vCenter soll keine Ereignisse oder Alarme an betroffene vCenter weiterleiten.
Alle Ereignisse anzeigen	Anzeigen aller Ereignisse, einschließlich informeller Ereignisse, die das OpenManage Integration for VMware vCenter von den verwalteten Dell Hosts der betroffenen vCenter erhält.
Nur kritische Ereignisse und Warnungsereignisse anzeigen	Veröffentlicht nur kritische Ereignisse und Warnungen an die entsprechenden vCenter.
Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen.	Veröffentlicht von Hosts empfangene Virtualisierung-bezogene Ereignisse an die entsprechenden vCenter. Virtualisierung-bezogene Ereignisse sind solche Ereignisse, in denen Dell für Hosts, die virtuelle Maschinen ausführen, die höchste Priorität zugewiesen hat.

Wenn Sie Ereignisse und Alarme konfigurieren, können Sie sie aktivieren. In diesem Fall führen kritische Hardware-Alarme dazu, dass das OpenManage Integration for VMware vCenterdas Hostsystem in den Wartungsmodus versetzt und die virtuellen Maschinen in bestimmten Fällen auf ein anderes Hostsystem migriert. Das OpenManage Integration for VMware vCenter leitet die von verwalteten Dell-Hosts empfangenen Ereignisse weiter und erstellt Alarme für diese Ereignisse. Sie können diese Alarme dazu verwenden, Aktionen des vCenter wie einen Neustart, den Wartungsmodus oder eine Migration zu veranlassen. Beispiel: Wenn eine duale Netzversorgung ausfällt und ein Alarm erzeugt wird, kann die virtuelle Maschine auf diesem Host auf einen anderen migriert werden.

Ein Host wechselt nur auf Anforderung in den oder aus dem Wartungsmodus. Befindet sich der Host beim Eintritt in den Wartungsmodus in einem Cluster, haben Sie die Möglichkeit, ausgeschaltete virtuelle Maschinen zu evakuieren. Ist diese Option ausgewählt, wird jede ausgeschaltete virtuelle Maschine auf einen anderen Host migriert, es sei denn, im Cluster steht kein kompatibler Host für die virtuelle Maschine zur Verfügung. Im Wartungsmodus erlaubt der Host keine Bereitstellung bzw. kein *Einschalten* einer virtuellen Maschine. Virtuelle Maschinen, die auf einem Host ausgeführt werden, der in den Wartungsmodus eintritt, werden entweder manuell oder automatisch vom VMware Distributed Resource Scheduling (DRS) auf einen anderen Host migriert oder heruntergefahren.

Alle Hosts außerhalb oder innerhalb der Cluster ohne aktiviertes VMware Distributed Resource Scheduling (DRS) können virtuelle Maschinen sehen, die aufgrund eines kritischen Ereignisses heruntergefahren werden. Das DRS überwacht die Nutzung kontinuierlich über einen Ressourcen-Pool und teilt verfügbare Ressourcen gemäß den Geschäftsanforderungen intelligent zwischen den virtuellen Maschinen auf. Verwenden Sie Cluster mit konfiguriertem DRS zusammen mit Dell-Alarmen, um sicherzustellen, dass virtuelle Maschinen bei kritischen Hardware-Ereignissen automatisch migriert werden. In den Details der Bildschirm-Meldungen werden alle eventuell betroffenen Cluster in dieser vCenter-Instanz aufgeführt. Bestätigen Sie, dass die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die Standard-Alarmeinstellungen wiederherstellen müssen, können Sie auf die Schaltfläche „Reset Default Alarm" (Standard-Alarmeinstellungen wiederherstellen) klicken. Mit dieser Schaltfläche kann die standardmäßige Alarm-Konfiguration wiederhergestellt werden, ohne dass das Produkt de- und neuinstalliert werden muss. Alle nach der Installation geänderten Dell-Alarm-Konfigurationen werden durch Klicken auf diese Schaltfläche auf die Standardeinstellung zurückgesetzt.



ANMERKUNG: Das OpenManage Integration for VMware vCenter trifft eine Vorauswahl der erforderlichen Virtualisierung-bezogenen Ereignisse, damit Hosts virtuelle Maschinen erfolgreich ausführen können. Die Dell-Host Alarme sind in der Standardeinstellung deaktiviert. Wenn die Dell-Alarme aktiviert werden, sollten die Cluster das VMware Distributed Resource Scheduling verwenden, um sicherzustellen, dass virtuelle Maschinen, die kritische Ereignisse senden, automatisch migriert werden.

Verstehen von Ereignissen und Warnmeldungen für Gehäuse

Ereignis- und Alarme zu einem Gehäuse werden nur auf vCenter-Ebene angezeigt. Ereignis- und Alarmeinstellungen, die für Hosts an jedem vCenter vorgenommen werden, betreffen auch die Gehäuseebene. Sie können die Ereignis- und Alarmeinstellungen aus OpenManage Integration for VMware vCenter in der Registerkarte **Verwalten** → **Einstellungen**bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für Dell-Hosts und -Gehäuse aktivieren oder Standardalarme wiederherstellen. Sie können die Ereignisse und Alarme für einzelne vCenter oder für alle registrierten vCenter alle gleichzeitig konfigurieren.



ANMERKUNG: Um Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

Viewing Chassis Events

```
Viewing Chassis Events
```

Wählen Sie im linken Fensterbereich „vCenter" aus und klicken Sie auf vCenter Server

Klicken Sie auf ein bestimmtes vCenter.

Klicken Sie auf der Registerkarte „Überwachen" auf Ereignisse.

Wählen Sie ein spezifisches Ereignis aus, um weitere Ereignisdetails anzeigen zu lassen.

Anzeigen von Gehäusealarmen

Wählen Sie im linken Fensterbereich „vCenter" aus und klicken Sie auf vCenter Server

Klicken Sie auf ein bestimmtes vCenter.

Die Alarme werden angezeigt. Es werden nur die ersten 4 Alarme angezeigt. Klicken Sie auf „Alle anzeigen" und die detaillierte Liste wird in der Registerkarte „Überwachen" als „Alle Probleme" angezeigt..

Klicken Sie auf den Alarm in **Ausgelöste Alarme** zur Anzeige der Alarmdefinition.

Anzeigen der Datenabrufzeitpläne für Bestandsaufnahme und Garantie

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten** → **Einstellungen** unter vCenter-Einstellungen auf **Zeitplan für den Abruf von Daten**.

   Der „Zeitplan für den Abruf von Garantiedaten" wird bei Anklicken erweitert, um die Zeitpläne für die Bestandsaufnahme und Garantie aufzudecken.
2. Lassen Sie die Einstellungen für Bestandsaufnahme oder Garantieabfrage anzeigen:

   - Zeigt an, ob die Option aktiviert oder deaktiviert ist
   - Zeigt die Wochentage an, für die sie aktiviert ist.
   - Zeigt die Tageszeit an, zu der sie aktiviert ist.
3. Wenn Sie erneut auf **Zeitplan für den Abruf von Garantiedaten** klicken, werden die Informationen auf eine einzelne Zeile eingerollt (eingeklappt) und es wird angezeigt, ob die Option aktiviert oder deaktiviert ist.
4. Wenn Sie den Zeitplan für den Abruf von Garantiedaten ändern wollen, dann lesen Sie Bestandsaufnahmen-Jobzeitpläne ändern oder Ändern eines Garantie-Jobzeitplans.

Verwendung von OMSA mit Servern der 11. Generation verstehen

Auf Servern vor der 12. Dell PowerEdge-Generation muss OMSA installiert werden, damit Dell OpenManage Integration for VMware vCenter ordnungsgemäß funktioniert. OMSA wird auf Dell PowerEdge-Hosts der 11. Generation automatisch im Rahmen der Bereitstellung installiert, Sie können jedoch immer noch eine manuelle Installation durchführen, falls Sie dies wünschen.

Wählen Sie für die Konfiguration von OMSA auf Dell PowerEdge-Hosts der 11. Generation unter den folgenden Optionen aus:

- Bereitstellen eines OMSA-Agenten auf einem ESXi-System
- Bereitstellen eines OMSA-Agenten auf einem ESX-System
- Einrichten eines OMSA-Trap-Ziels



ANMERKUNG: Abgesehen von den oben genannten Optionen können Sie den .NET-Client verwenden und die Option „Host-Konformität" ausführen. Auf diese Weise können Sie den OMSA-Agenten installieren und konfigurieren.

Bereitstellen eines OMSA-Agenten auf einem ESXi-System

Installieren Sie den OMSA VIB auf einem ESXi-System, um eine Bestandsliste und Alarminformationen von den Systemen zu erstellen.



ANMERKUNG: OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. Falls noch nicht geschehen, installieren Sie das vSphere-Befehlszeilentool (vSphere CLI) von **http://www.vmware.com**.
2. Geben Sie folgenden Befehl ein:

   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
   ```

   ANMERKUNG: Die Installation von OMSA kann einige Minuten dauern. Dieser Befehl erfordert einen Neustart des Hosts nach Abschluss der Installation.

Bereitstellen eines OMSA-Agenten auf einem ESX-System

Installieren Sie die OMSA-Datei tar.gz auf einem ESX-System, um eine Bestandsliste und Alarminformationen der Systeme zu erstellen.



ANMERKUNG: OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

So stellen Sie die OMSA-Agent-Datei tar.gz auf einem ESX-System mit der erforderlichen Remote-Aktivierungseinstellung (-c) bereit:

1. Führen Sie das OMSA-Agent-Installationsskript aus:
   ```
   srvadmin-install.sh -x -c
   ```
2. Starten Sie die OMSA-Dienste:
   ```
   srvadmin-services.sh start
   ```
3. Wenn der OMSA-Agent bereits installiert wurde, stellen Sie sicher, dass die Remote-Aktivierungseinstellung (-c) konfiguriert ist, anderenfalls kann die Installation des OpenManage Integration for VMware vCenter nicht erfolgreich abgeschlossen werden. Installieren Sie sie mit der Option -c erneut und starten Sie den Dienst neu:
   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

Einrichten eines OMSA-Trap-Ziels

Diese Aufgabe ist nur für Hostsysteme erforderlich, die OMSA anstelle von iDRAC6 zum Erzeugen von Ereignissen verwenden. Für iDRAC6 ist keine zusätzliche Konfiguration erforderlich.



ANMERKUNG: OMSA ist nur auf Dell-Servern erforderlich, die älter als die 12. Dell PowerEdge-Server-Generation sind.

1. Verwenden Sie entweder den Link zur OMSA-Benutzeroberfläche in der Registerkarte OpenManage Integration for VMware vCenter **Einstellungen** → **verwalten**, oder navigieren Sie mittels eines Webbrowsers zum OSMA-Agenten (**https://<HostIP>:1311/**).
2. Melden Sie sich an und wählen Sie die Registerkarte **Alarmverwaltung**.
3. Wählen Sie **Alarm-Aktionen** und stellen Sie sicher, dass die Option **Broadcast-Nachricht** für alle zu überwachenden Ereignisse gesetzt ist, so dass die Ereignisse gesendet werden.
4. Wählen Sie oben auf der Registerkarte die Option **Plattformereignisse** aus.
5. Klicken Sie auf die graue Schaltfläche **Ziele konfigurieren** und dann auf den Link **Ziel**.
6. Aktivieren Sie das Kontrollkästchen **Ziel aktivieren**.
7. Geben Sie die OpenManage Integration for VMware vCenter Geräte-IP-Adresse in das Feld **Ziel-IP-Adresse** ein.
8. Klicken Sie auf **Änderungen anwenden**.
9. Wiederholen Sie die Schritte 1 bis 8, um weitere Ereignisse zu konfigurieren.

8

Anzeigen der Garantieablaufbenachrichtigungseinstellungen

1. Klicken Sie im OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen**unter Geräteeinstellungen auf **Garantieablaufbenachrichtigung**.
2. Unter Garantieablaufbenachrichtigung können Sie folgendes anzeigen lassen:
   - Aktivierungs- oder Deaktivierungsstatus der Einstellung.
   - Einstellung der Anzahl der Tage bis zur ersten Warnung.
   - Einstellung der Anzahl der Tage bis zur krtischen Warnung.
3. Lesen Sie für die Konfiguration der Garantieablaufbenachrichtigung Garantieablaufbenachrichtigungseinstellungen konfigurieren.

Garantieablaufbenachrichtigung anzeigen

Sie können Garantieablaufschwellenwerte konfigurieren, die Sie über den Ablauf der Garantie informieren.

1. Klicken Sie im OpenManage Integration for VMware vCenter auf dem Register **Verwalten** → **Einstellungen**unter Geräteeinstellungen auf der rechten Seite von **Garantieablaufbenachrichtigung** auf das Symbol **Bearbeiten**.
2. Verfahren Sie im Dialogfeld „Garantieablaufinformationen" wie folgt:
   a. Falls Sie diese Einstellung aktivieren möchten, markieren Sie das Kontrollkästchen **Garantieablaufbenachrichtigung für Hosts aktivieren**.

      Das Wählen des Kontrollkästchens aktiviert die Garantieablaufbenachrichtigung.

   b. Verfahren Sie unter „Mindesttageschwellenwertalarm" wie folgt:

      1. Wählen Sie in der Drop-Down-Liste „Warnung" den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf der Garantie gewarnt werden wollen.
      2. Wählen Sie in der Drop-Down-Liste „Kritisch" den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf der Garantie gewarnt werden wollen.
3. Klicken Sie auf **Anwenden**.

9

Allgemeines zu Firmware-Aktualisierungen

Der Standort, auf dem Server Firmware-Aktualisierungen erhalten, ist eine globale Einstellung, die im OpenManage Integration for VMware vCenter im Register „Einstellungen“ verfügbar ist.

Die Einstellungen für das Firmware-Repository enthalten den Speicherort des Firmware-Katalogs, der zum Aktualisieren von bereitgestellten Servern verwendet wird. Es gibt zwei Arten von Speicherorten:

Dell (ftp.dell.com)	Verwendet das Repository zur Firmware-Aktualisierung von Dell (**ftp.dell.com**). OpenManage Integration for VMware vCenterr lädt die ausgewählten Firmware-Aktualisierungen von Dell herunter.
Freigegebene Netzwerkordner	Erstellt mit Dell Repository Manager™. Diese lokalen Repositorien befinden sich auf der CIFS- oder der NFS-Dateifreigabe.



ANMERKUNG: Nachdem ein Repository erstellt wurde, speichern Sie es an einem Speicherort, auf den registrierte Hosts zugreifen können. Die Kennwörter für Repositorien dürfen nicht mehr als 31 Zeichen umfassen. Folgende Zeichen dürfen dabei nicht verwendet werden: @, &, %, ', ", ,(Komma), < >

Der Assistent zur Aktualisierung der Firmware prüft stets die erforderlichen Mindest-Firmware-Versionen für iDRAC, BIOS und den Lifecycle Controller und versucht, diese auf die erforderlichen Mindestversionen zu aktualisieren. Wenn die iDRAC-, Lifecycle- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Assistent zur Aktualisierung der Firmware alle Firmware-Aktualisierungen, einschließlich iDRAC, Lifecycle Controller, RAID, NIC/LOM, Netzteile, BIOS usw.



ANMERKUNG: Bei Servern der 9. und 10. Generation können die BIOS/BMC/DRAC-Firmware-Versionen nur auf der „Cluster View“-Ebene in vCenter oder auf der Seite „Übersicht“ in der individuellen Hostansicht angezeigt werden. Die Informationen zur Firmware-Version sind in der individuellen Hostansicht unter „Firmware“ nicht aktiv und remote Firmware-Aktualisierungen stehen nicht zur Verfügung.

Firmware-Versionen nach dem 14. Oktober 2010

Bei Firmware, die am oder nach dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware ausgeführt.

Firmware-Versionen neuer als 29. Juli 2009 und vor dem 14. Okober 2010

Wenn Ihre Firmware am oder nach dem 29. Juli 2009 und vor dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware nicht angezeigt, stattdessen erhalten Sie ein ISO-Paket zur Aktualisierung Ihrer Firmware. Auch nach dieser Aktualisierung verfügen Sie eventuell noch nicht über die aktuellste Firmware. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Firmware-Versionen vor 29. Juli 2009

Wenn Ihre Firmware älter als 29. Juli 2009 ist, müssen Sie die ISO-Datei herunterladen und ausführen, um Ihre Maschinen zu aktualisieren. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Weitere Informationen:

- Einrichten des Firmware-Repositorys

Einrichten des Firmware-Aktualisierungs-Repositorys

Sie können das Repository für die Firmwareaktualisierung auf der Registerkarte der Einstellungen für OpenManage Integration for VMware vCenter einrichten.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf dem Register **Verwalten** → **Einstellungen** unter Geräteeinstellungen und auf der rechten Seite des Repository für die Firmwareaktualisierung auf das Symbol **Bearbeiten**.
2. Wählen Sie im Dialogfeld Firmware-Aktualisierungs-Repository eine der folgenden Optionen aus:
   - Dell Online

     Standard-Firmware-Repository (ftp.dell.com) mit einem Arbeitsordner. Die OpenManage Integration for VMware vCenter lädt ausgewählte Firmwareaktualisierungen herunter und speichert sie im Arbeitsordner, und dann müssen Sie den Firmwareassistenten ausführen, um die Firmware zu aktualisieren.
   - Freigegebene Netzwerkordner

     Diese werden mit der Anwendung Dell Repository Manager erstellt. Sie finden diese lokalen Repositorys auf windowsbasierten Dateifreigaben. Verwenden Sie den Live-Link, um zum Dell Repository Manager zu gehen.
3. Wenn Sie **Freigegebenen Netzwerkordner** ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie den **Speicherort der Katalogdatei** in der folgenden Syntax ein:
      - NFS-Freigabe für xml-Datei: host:/share/filename.xml
      - NFS-Freigabe für gz-Datei: host: /share/filename.gz
      - CIFS-Freigabe für xml-Datei: \\host\share/filename.xml
      - CIFS-Freigabe für gz-Datei: \\host\share/filename.gz

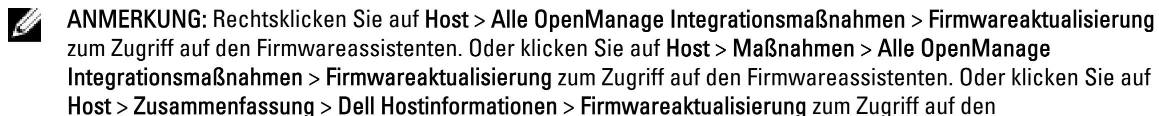
   b. Falls das Herunterladen der Dateien im ausgewählten Repository-Pfad läuft, der auf dem Bildschirm **Aktualisierungsquelle auswählen** angezeigt wird, wird eine Fehlermeldung angezeigt, die besagt, dass der Download läuft.
4. Wenn das Herunterladen der Datei abgeschlossen ist, klicken Sie auf **Anwenden**.

Ausführen des Firmwareaktualisierungsassistenten für einen einzelnen Host

Diese Funktionalität steht nur für die 11., 12. und 13. Generation von Dell-Servern zur Verfügung, die entweder eine iDRAC Express- oder eine Enterprise-Karte haben. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversion automatisch mit dem Firmware-Update-Assistenten aktualisieren.



ANMERKUNG: Ändern Sie zum Schutz gegen Fehler durch Zeitüberschreitung des Browsers die Standardzeit auf 30 Sekunden. Weitere Informationen zum Ändern der Standardzeitüberschreitungseinstellungen finden Sie unter „Warum wird eine Fehlermeldung nachdem ich auf den Firmware-Aktualisierungslink geklickt habe, angezeigt?“ im Abschnitt „Fehlerbehebung“ im *Benutzerhandbuch*.



ANMERKUNG: Rechtsklicken Sie auf **Host** > **Alle OpenManage Integrationsmaßnahmen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten. Oder klicken Sie auf **Host** > **Maßnahmen** > **Alle OpenManage Integrationsmaßnahmen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten. Oder klicken Sie auf **Host** > **Zusammenfassung** > **Dell Hostinformationen** > **Firmwareaktualisierung** zum Zugriff auf den Firmwareassistenten.

So führen Sie den Firmware-Update-Assistenten aus:

1. Klicken Sie im **vSphere Web-Client** auf **Hosts**. Die Liste verfügbarer Hosts wird angezeigt.
2. Wählen Sie einen Host aus der angezeigten Liste aus.

3. Klicken Sie im Hauptmenü auf **Überwachen** und wählen Sie dann die Registerkarte **Dell-Hostinformationen**. Die Bestandsaufnahmedaten der Dell-Hosts werden angezeigt.
4. Klicken Sie auf **Firmware**, und die verfügbaren Firmwareversionen mit den Details werden angezeigt.
5. Klicken Sie auf **Firmwareassistent ausführen**. Der Bildschirm **Firmwareaktualisierung** wird angezeigt.
6. Klicken Sie auf **Weiter**. Daraufhin wird der Bildschirm **Aktualisierungsquelle auswählen** mit dem Firmware-Aktualisierungsbündel für den angegebenen Host angezeigt. Wählen Sie auf dem Bildschirm das Firmware-Aktualisierungsbündel aus der Dropdown-Liste **Ein Aktualisierungsbündel auswählen** aus.
7. Klicken Sie auf **Weiter**. Der Bildschirm **Komponenten auswählen** wird angezeigt. Dieser listet die Firmwaredetails für die Komponenten auf.
8. Wählen Sie die gewünschten Firmwareaktualisierungen aus und klicken Sie auf **Weiter**. Komponenten, die zurückgestuft wurden, bereits aktuell sind oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Falls Sie das Kontrollkästchen **Zurückstufung der Firmware gestatten** markieren, wählen Sie die Optionen aus, die als Zurückstufung aufgeführt sind. Die Auswahl dieser Option ist nur fortgeschrittenen Benutzern empfohlen, die die Folgen einer Zurückstufung der Firmware verstehen.
9. Klicken Sie auf **Weiter.** Der Bildschirm **Firmwareaktualisierung planen** wird angezeigt.
   - Geben Sie den Jobnamen im Feld **Jobname der Firmwareaktualisierung** und die Beschreibung im Feld **Beschreibung der Firmwareaktualisierung** ein. Diese Feldeingabe ist optional.
   - Wählen Sie **Jetzt aktualisieren** zum sofortigen Start der Firmwareaktualisierung.
   - **Aktualisierung planen**, wählen Sie diese Schaltfläche aus, um den Firmwareaktualisierungsjob später auszuführen, und klicken Sie auf **Weiter**. Sie können den Firmwareaktualisierungsjob für 30 Minuten nach der aktuellen Uhrzeit planen.
   - Wählen Sie im Kontrollkästchen Kalender den Monat und Tag aus.
   - Geben Sie im Textfeld „Zeit" die Uhrzeit im Format HH:MM ein, und klicken Sie dann auf „Weiter". Die Uhrzeit entspricht der lokalen Ortszeit, wo Ihr Client sich physisch befindet. Ungültige Zeitwerte könnten zu einer blockierten Aktualisierung führen.
   - **Wenden Sie die Aktualisierungen beim nächsten Neustart an.**

     Um eine Dienstunterbrechung zu vermeiden, wird empfohlen, dass der Host vor dem Neustart in den Wartungsmodus übergeht.
   - **Aktualisierungen anwenden und den Neustart erzwingen, ohne in den Wartungsmodus überzugehen.**

     Die Aktualisierung wird angewandt, und ein Neustart wird ausgeführt, auch wenn der Host nicht im Wartungsmodus ist. Diese Methode ist nicht empfehlenswert.
10. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Details über alle Komponenten nach der Firmwareaktualisierung bereit.
11. Klicken Sie auf **Fertigstellen**.
12. Um zu überprüfen, dass die Aktualisierung erfolgreich verlaufen ist, wählen Sie im Register **Überwachen Job-Warteschlange → Firmwareaktualisierungen** und überprüfen Sie die Seite **OpenManage Integration-Übersicht**, um die neuen Versionen zu sehen.

Ausführen des Firmwareaktualisierungsassistenten für einen Cluster

Diese Funktion steht nur für Dell-Server der 11., 12. und 13. Generation zur Verfügung, die eine iDRAC Express- oder eine Enterprise-Karte haben. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversionen automatisch mit dem Firmwareaktualisierungsassistenten aktualisieren. Dieser Assistent aktualisiert nur Hosts, die Teil eines Verbindungsprofils sind und in Bezug auf Firmware, CSIOR-Status, Hypervisor und OMSA-Status (nur Server der 11. Generation) konform sind. Wählen Sie einen Cluster, der in der Clusteransicht aufgelistet ist, und verwenden Sie den Firmwareaktualisierungsassistenten. Es dauert normalerweise 30 bis 60 Minuten, um die Firmwarekomponenten aller Cluster zu aktualisieren. Aktivieren Sie DRS auf einem Cluster, damit virtuelle Maschinen migriert werden können, wenn ein Host den Wartungsmodus während der Firmwareaktualisierung betritt/verlässt. Sie können nur einen Firmwareaktualisierungs-Task auf einmal planen oder ausführen.

Verwenden Sie zum Export aus dem Assistenten die CSV-Taste. Die Suche steht für das Lokalisieren eines bestimmten Clusters, Datenzetrums, Host oder jeden Themenpunkt der Datentabelle außer für „Datum der Anwendung“ zur Verfügung.

 **ANMERKUNG:** Aktualisieren Sie die Firmware immer zusammen als Teil des Repository-Pakets: BIOS, iDRAC und Lifecycle Controller.

 **ANMERKUNG:** Informationen über das Ändern der standardmäßigen Zeitüberschreitungseinstellung finden Sie im Abschnitt 'Fehlerbehebung' im *Benutzerhandbuch*.

Sie können den Status der Firmware-Aktualisierungs-Jobs auf der Seite „Job-Warteschlange“ anzeigen und verwalten. Siehe Anzeige von Firmware-Aktualisierungen für Cluster und Datenzentren.

1. Klicken Sie auf das Symbol **OpenManage Integration,** dann auf **Cluster,** angezeigt im linken Bereich. Die Liste von Clustern wird angezeigt.
2. Klicken Sie auf einen Cluster in der angezeigten Liste. Das Hauptmenü wird mit verschiedenen Optionen angezeigt.
3. Klicken Sie auf **Überwachen** -->**Dell Clusterinformationen** -->**Firmware**. Der Bildschirm **Firmwareassistent ausführen** wird angezeigt.
4. Klicken Sie auf den Link **Firmwareassistent ausführen**. Die Seite **Willkommen** wird angezeigt.
5. Klicken Sie auf **Weiter**. Der Bildschirm **Aktualisierungsquelle auswählen** wird angezeigt; hier können Sie die Bündel auswählen. Der Repository-Standort wird auch angezeigt.
6. Wählen Sie den Host aus der angezeigten Liste im Bereich **Bündel auswählen** aus. Sie sollten mindestens ein Bündel für die Firmwareaktualisierung auswählen. Neben jedem Host gibt es eine Dropdown-Liste neben dem Hostnamen, aus der Sie das erforderliche Bündel auswählen können.
7. Klicken Sie auf **Weiter**. Der Bildschirm **Komponenten auswählen** wird angezeigt. Dieser Bildschirm enthält die Details von Komponenten, wie u. a. Modellname, Hostname, Service-Tag-Nummer, Komponente usw. für den ausgewählten Host.
8. Wählen Sie mindestens eine Komponente aus der Liste aus, und klicken Sie zum Fortfahren auf **Weiter**. Sie können den Inhalt des Komponentendatengitters mit dem Feld **Filtern** filtern oder Spalten innerhalb des Komponentendatengitters verschieben. Falls Sie das Kontrollkästchen **Firmwareherabstufung zulassen** markieren, wird die vorhandene Firmwareversion auf die vorherige verfügbare Version zurückgestuft.
9. Klicken Sie auf **Weiter**, und der Bildschirm **Firmwareaktualisierung planen** wird angezeigt.
   a. Geben Sie den Namen des Firmwareaktualisierungs-Jobs im Feld **Firmwareaktualisierungs-Jobname** ein. Dieser Wert ist obligatorisch.
   b. Geben Sie die Beschreibung der Firmwareaktualisierung im Feld **Firmwareaktualisierungsbeschreibung** ein. Dieser Wert ist optional.
10. Wählen Sie eine der folgenden Optionen aus.
    a. **Jetzt aktualisieren**, wählen Sie diese Schaltfläche aus, um den Firmwareaktualisierungsjob jetzt auszuführen, und klicken Sie auf **Weiter**.
    b. **Aktualisierung planen**: Wählen Sie diese Schaltfläche aus, um den Firmware-Aktualisierungsjob später auszuführen, und klicken Sie auf **Weiter**. Sie können den Firmware-Aktualisierungsjob für 30 Minuten nach der aktuellen Uhrzeit planen.
    c. Wählen Sie im Kontrollkästchen **Kalender** den Monat und Tag aus.
    d. Geben Sie im Textfeld **Zeit** die Uhrzeit im Format HH:MM ein, und klicken Sie dann auf **Weiter**. Die Uhrzeit ist die Ortszeit, wo Ihr Client sich befindet. Ungültige Zeitwerte führen zu einer blockierten Aktualisierung.
11. Der Bildschirm **Zusammenfassung** wird mit allen Firmwareaktualisierungsdetails angezeigt.
12. Klicken Sie auf **Fertig stellen,** und die Meldung **Der Firmwareaktualisierungsjob wurde erstellt** wird für die erfolgreiche Firmwareaktualisierung angezeigt.

10 Verstehen von Ereignissen und Warnmeldungen für Hosts

Sie können Ereignisse und Alarmeinstellungen von OpenManage Integration for VMware vCenter aus innerhalb der Registerkarte **Verwalten** → **Einstellungen**bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für Dell Hosts aktivieren oder Standardalarme wiederherstellen. Sie können Ereignisse oder Alarme für einzelne vCenter oder alle registrierten vCenter gleichzeitig konfigurieren.

Es gibt vier Ereignis-Veröffentlichungsstufen.

Tabelle 3. Beschreibung der Ereignis-Veröffentlichungsstufen

Ereignis	Beschreibung
Keine Ereignisse anzeigen	OpenManage Integration for VMware vCenter soll keine Ereignisse oder Alarme an betroffene vCenter weiterleiten.
Alle Ereignisse anzeigen	Anzeigen aller Ereignisse, einschließlich informeller Ereignisse, die das OpenManage Integration for VMware vCenter von den verwalteten Dell Hosts der betroffenen vCenter erhält.
Nur kritische Ereignisse und Warnungsereignisse anzeigen	Veröffentlicht nur kritische Ereignisse und Warnungen an die entsprechenden vCenter.
Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen.	Veröffentlicht von Hosts empfangene Virtualisierung-bezogene Ereignisse an die entsprechenden vCenter. Virtualisierung-bezogene Ereignisse sind solche Ereignisse, in denen Dell für Hosts, die virtuelle Maschinen ausführen, die höchste Priorität zugewiesen hat.

Wenn Sie Ereignisse und Alarme konfigurieren, können Sie sie aktivieren. In diesem Fall führen kritische Hardware-Alarme dazu, dass das OpenManage Integration for VMware vCenterdas Hostsystem in den Wartungsmodus versetzt und die virtuellen Maschinen in bestimmten Fällen auf ein anderes Hostsystem migriert. Das OpenManage Integration for VMware vCenter leitet die von verwalteten Dell-Hosts empfangenen Ereignisse weiter und erstellt Alarme für diese Ereignisse. Sie können diese Alarme dazu verwenden, Aktionen des vCenter wie einen Neustart, den Wartungsmodus oder eine Migration zu veranlassen. Beispiel: Wenn eine duale Netzversorgung ausfällt und ein Alarm erzeugt wird, kann die virtuelle Maschine auf diesem Host auf einen anderen migriert werden.

Ein Host wechselt nur auf Anforderung in den oder aus dem Wartungsmodus. Befindet sich der Host beim Eintritt in den Wartungsmodus in einem Cluster, haben Sie die Möglichkeit, ausgeschaltete virtuelle Maschinen zu evakuieren. Ist diese Option ausgewählt, wird jede ausgeschaltete virtuelle Maschine auf einen anderen Host migriert, es sei denn, im Cluster steht kein kompatibler Host für die virtuelle Maschine zur Verfügung. Im Wartungsmodus erlaubt der Host keine Bereitstellung bzw. kein *Einschalten* einer virtuellen Maschine. Virtuelle Maschinen, die auf einem Host ausgeführt werden, der in den Wartungsmodus eintritt, werden entweder manuell oder automatisch vom VMware Distributed Resource Scheduling (DRS) auf einen anderen Host migriert oder heruntergefahren.

Alle Hosts außerhalb oder innerhalb der Cluster ohne aktiviertes VMware Distributed Resource Scheduling (DRS) können virtuelle Maschinen sehen, die aufgrund eines kritischen Ereignisses heruntergefahren werden. Das DRS überwacht die Nutzung kontinuierlich über einen Ressourcen-Pool und teilt verfügbare Ressourcen gemäß den Geschäftsanforderungen intelligent zwischen den virtuellen Maschinen auf. Verwenden Sie Cluster mit konfiguriertem DRS zusammen mit Dell-Alarmen, um sicherzustellen, dass virtuelle Maschinen bei kritischen Hardware-Ereignissen automatisch migriert werden. In den Details der Bildschirm-Meldungen werden alle eventuell betroffenen Cluster in dieser vCenter-Instanz aufgeführt. Bestätigen Sie, dass die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die Standard-Alarmeinstellungen wiederherstellen müssen, können Sie auf die Schaltfläche „Reset Default Alarm“ (Standard-Alarmeinstellungen wiederherstellen) klicken. Mit dieser Schaltfläche kann die standardmäßige Alarm-Konfiguration wiederhergestellt werden, ohne dass das Produkt de- und neuinstalliert werden muss. Alle nach der Installation geänderten Dell-Alarm-Konfigurationen werden durch Klicken auf diese Schaltfläche auf die Standardeinstellung zurückgesetzt.



ANMERKUNG: Das OpenManage Integration for VMware vCenter trifft eine Vorauswahl der erforderlichen Virtualisierung-bezogenen Ereignisse, damit Hosts virtuelle Maschinen erfolgreich ausführen können. Die Dell-Host Alarme sind in der Standardeinstellung deaktiviert. Wenn die Dell-Alarme aktiviert werden, sollten die Cluster das VMware Distributed Resource Scheduling verwenden, um sicherzustellen, dass virtuelle Maschinen, die kritische Ereignisse senden, automatisch migriert werden.

Verstehen von Ereignissen und Warnmeldungen für Gehäuse

Ereignis- und Alarme zu einem Gehäuse werden nur auf vCenter-Ebene angezeigt. Ereignis- und Alarmeinstellungen, die für Hosts an jedem vCenter vorgenommen werden, betreffen auch die Gehäuseebene. Sie können die Ereignis- und Alarmeinstellungen aus OpenManage Integration for VMware vCenter in der Registerkarte **Verwalten → Einstellungen**bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für Dell-Hosts und -Gehäuse aktivieren oder Standardalarme wiederherstellen. Sie können die Ereignisse und Alarme für einzelne vCenter oder für alle registrierten vCenter alle gleichzeitig konfigurieren.



ANMERKUNG: Um Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

Viewing Chassis Events

```
Viewing Chassis Events
```

Wählen Sie im linken Fensterbereich „vCenter“ aus und klicken Sie auf vCenter Server

Klicken Sie auf ein bestimmtes vCenter.

Klicken Sie auf der Registerkarte „Überwachen“ auf Ereignisse.

Wählen Sie ein spezifisches Ereignis aus, um weitere Ereignisdetails anzeigen zu lassen.

Anzeigen von Gehäusealarmen

Wählen Sie im linken Fensterbereich „vCenter“ aus und klicken Sie auf vCenter Server

Klicken Sie auf ein bestimmtes vCenter.

Die Alarme werden angezeigt. Es werden nur die ersten 4 Alarme angezeigt. Klicken Sie auf „Alle anzeigen“ und die detaillierte Liste wird in der Registerkarte „Überwachen“ als „Alle Probleme“ angezeigt..

Klicken Sie auf den Alarm in **Ausgelöste Alarme** zur Anzeige der Alarmdefinition.

Konfigurieren von Ereignissen und Alarmen

Detaillierte Informationen über Ereignisse und Alarme finden Sie unter Verstehen von Alarmen und Ereignissen. Konfigurieren Sie Ereignisse und Alarme auf der Registerkarte OpenManage Integration for VMware vCenter **Verwaltungs → einstellungen**. Unter vCenter-Einstellungen erweitern Sie die Überschrift „Ereignisse und Alarme“, um die aktuellen vCenter-Alarme für Dell-Hosts (aktiviert oder deaktiviert) anzuzeigen, oder für alle und die Ereignisanzeigeebene.



ANMERKUNG: Bei Hosts vor der Version der Dell PowerEdge-Server der 12. Generation erfordert diese Funktion, dass das virtuelle Gerät als ein Trap-Ziel in OMSA konfiguriert ist, um Host-Ereignisse im vCenter anzuzeigen. Weitere Informationen zu OMSA finden Sie unter Einrichten eines OMSA Trap-Zieles.



ANMERKUNG: Um Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

1. Auf der Registerkarte OpenManage Integration for VMware vCenter **Verwalten** → **Einstellungen** neben den vCenter-Einstellungen verwenden Sie die Dropdown-Liste zur Auswahl des vCenter-Servers oder aller vCenter-Server, die in dieser Einstellung eingeschlossen sind.

   Falls Sie „Alle registrierten Server“ ausgewählt haben, werden die Optionen evtl. leer angezeigt. Dies ermöglicht Ihnen die Konfiguration der Einstellungen für alle registrierten vCenters auf einmal. Falls die vCenters dieselben Einstellungen haben, werden diese angezeigt.
2. Klicken Sie auf der rechten Seite von „Ereignisse und Alarme“ auf das Symbol **Bearbeiten**.
3. Aktivieren Sie das Kontrollkästchen **Alarme für alle Dell-Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Dell-Hosts mit aktivierten Alarmen reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus übergehen, und Sie können den Alarm nach Bedarf ändern.
4. Klicken Sie auf **Standard Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.
5. Wählen Sie eine der folgenden Optionen unter **Übermittlungsebene für das Ereignis**:

   - Keine Ereignisse anzeigen

     Diese Option blockiert Hardware-Ereignisse.
   - Alle Ereignisse anzeigen

     Diese Option veröffentlicht alle Hardware-Ereignisse.
   - Nur kritische Ereignisse und Warnungsereignisse anzeigen

     Diese Option veröffentlicht nur kritische Hardwareereignisse oder Ereignisse mit Warnungsstufe.
   - Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen.

     Diese Option veröffentlicht nur virtualisierungsbezogene kritische Ereignisse und Warnungsereignisse. Dies ist die standardmäßige Einstellung der Veröffentlichungsstufe.
6. Falls Sie diese Einstellungen auf alle vCenters anwenden möchten, markieren Sie das Kontrollkästchen **Diese Einstellungen auf alle vCenters anwenden**.

   ANMERKUNG: Die Auswahl dieser Option überschreibt die vorhandenen Einstellungen für alle vCenters.

   Diese Option ist ausgeblendet, wenn Sie bereits 'Alle registrierten vCenter' aus der Dropdown-Liste der Einstellungsseite ausgewählt haben.
7. Klicken Sie zum Speichern auf **Anwenden**.

Anzeigen von Ereignissen

Konfigurieren Sie Ereignisse, bevor Sie diese in der Registerkarte „Ereignisse“ anzeigen lassen können. Siehe Konfigurieren von Ereignissen und Alarmen.
Lassen Sie die Ereignisse für einen Host, Cluster oder Datacenter auf der Registerkarte „Ereignisse“ anzeigen.

1. Klicken Sie im Navigator des OpenManage Integration for VMware vCenter auf **Hosts**, **Datacenter** oder **Cluster**.
2. Wählen Sie auf der Registerkarte „Objekte“ einen spezifischen Host, ein Datacenter oder einen Cluster aus, für den Sie Ereignisse anzeigen lassen wollen.
3. Klicken Sie auf der Registerkarte „Überwachen“ auf **Ereignisse**.
4. Wählen Sie ein spezifisches Ereignis aus, um weitere Ereignisdetails anzeigen zu lassen.

Anzeigen der Alarm- und Ereigniseinstellungen

Sobald Alarme und Ereignisse konfiguriert wurden, können Sie anzeigen lassen, ob die vCenter-Alarme für Hosts aktiviert sind und welche Ereignisveröffentlichungsstufe auf der Registerkarte „Einstellungen“ ausgewählt wurde.

1. Erweitern Sie im Register OpenManage Integration for VMware vCenter**Verwalten** → **Einstellungen** unter „vCenter-Einstellungen“ „Ereignisse und Alarme“.
2. Unter „Ereignisse und Alarme“ können Sie folgendes anzeigen lassen:
   - vCenter-Alarme für Dell Hosts: zeigt entweder „Aktiviert“ oder „Deaktiviert“ an.
   - Ereignis-Veröffentlichungsstufe

     Lesen Sie für die anzeigbaren Ereignis-Veröffentlichungsstufen unter Ereignisse und Alarme verstehen nach.
3. Lesen Sie zum Konfigurieren von Alarmen und Ereignissen Konfigurieren von Alarmen und Ereignissen

Anzeigen der Datenabrufzeitpläne für Bestandsaufnahme und Garantie

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten** → **Einstellungen** unter vCenter-Einstellungen auf **Zeitplan für den Abruf von Daten**.

   Der „Zeitplan für den Abruf von Garantiedaten“ wird bei Anklicken erweitert, um die Zeitpläne für die Bestandsaufnahme und Garantie aufzudecken.
2. Lassen Sie die Einstellungen für Bestandsaufnahme oder Garantieabfrage anzeigen:
   - Zeigt an, ob die Option aktiviert oder deaktiviert ist
   - Zeigt die Wochentage an, für die sie aktiviert ist.
   - Zeigt die Tageszeit an, zu der sie aktiviert ist.
3. Wenn Sie erneut auf **Zeitplan für den Abruf von Garantiedaten** klicken, werden die Informationen auf eine einzelne Zeile eingerollt (eingeklappt) und es wird angezeigt, ob die Option aktiviert oder deaktiviert ist.
4. Wenn Sie den Zeitplan für den Abruf von Garantiedaten ändern wollen, dann lesen Sie Bestandsaufnahmen-Jobzeitpläne ändern oder Ändern eines Garantie-Jobzeitplans.

11 Anzeigen des zugeordneten Hosts für ein Gehäuse

Sie können Informationen über die zugeordneten Hosts für das ausgewählte Gehäuses auf der Seite **Verwalten** anzeigen.

So zeigen Sie Informationen zu dem zugeordneten Host an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Verwalten**.

   Die folgenden Informationen über den zugeordneten Host werden angezeigt:

   - Host-Name (Falls Sie auf die ausgewählten Host-IP-Adresse klicken, werden die Details zum Host angezeigt.)
   - Service-Tag-Nummer
   - Modell
   - iDRAC IP (iDRAC-IP)
   - Einschubposition
   - Letzte Bestandsaufnahme

12

Gehäuseverwaltung

OpenManage Integration für VMware vCenter ermöglicht Ihnen, zusätzliche Informationen für ein ausgewähltes Gehäuse anzuzeigen. Auf der Registerkarte „Gehäuseinformationen“ können Sie die Einzelheiten der Gehäuseübersicht für ein einzelnes Gehäuse, Informationen über die Hardware-Bestandsliste, Firmware und Verwaltungs-Controller anzeigen. Die folgenden drei Registerkarten werden für jedes Gehäuse angezeigt und unterscheiden sich bei manchen Gehäusen abhängig von den Gehäusemodellen.

Registerkarte **Zusammenfassung**

Registerkarte **Überwachen**

Registerkarte **Verwalten**

Anzeigen von Details der Gehäusezusammenfassung

Sie können die Details der Gehäusezusammenfassung für ein einzelnes Gehäuse auf der Seite der Gehäuse-**Zusammenfassung** anzeigen.

So zeigen Sie die Details der Gehäusezusammenfassung an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Zusammenfassung**.

   Die folgenden Informationen über das ausgewählte Gehäuse werden angezeigt:

   - Name
   - Modell
   - Firmware-Version
   - Service-Tag-Nummer
   - CMC (Wenn Sie auf den Link **CMC** klicken, wird die Seite „Chassis Management Controller“ angezeigt.)

   ANMERKUNG: Wenn Sie keine Gehäuse inventarisieren, sehen Sie nur die Service-Tag-Nummer und die CMC-IP-Adresse.

5. Sie können den Funktionszustand der dem ausgewählten Gehäuse zugeordneten Geräte anzeigen. Das Hauptfenster zeigt den Gesamtfunktionszustand eines Gehäuses an. Die gültigen Anzeigen des Funktionszustands lauten **Funktionsfähig**, **Warnung**, **Kritisch**, **Nicht vorhanden**. In der Rasteransicht **Gehäusefunktionszustand** wird der Funktionszustand jeder Komponente angezeigt. Die Funktionszustandsparameter von Gehäusen gelten für die Modelle **VRTX Version 1.0 und höher, M1000e Version 4.4 und höher**. Für Versionen unter 4.3 werden nur zwei Anzeigen angezeigt: **Fehlerfrei** und **Warnung oder Kritisch** (Umgekehrtes Dreieck mit einem Ausrufezeichen in orangener Farbe).

   ANMERKUNG: Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit dem niedrigsten Funktionszustandsparameter an. Wenn zum Beispiel 5 Zeichen für funktionsfähig und 1 Zeichen für Warnung vorhanden sind, wird der Gesamtfunktionszustand als Warnung angezeigt.

6. Sie können den CMC **Enterprise** oder **Express** mit dem Lizenztyp und dem Ablaufdatum für ein Gehäuse anzeigen. Dies gilt nicht für das M1000e-Gehäuse.
7. Im **Garantie**-Symbol werden die Anzahl der verbleibenden Tage und die verstrichenen Tage für einen Server angezeigt. Wenn Sie mehr als eine Garantie besitzen, wird der letzte Tag der letzten Garantie für die Berechnung der verbleibenden Garantietage verwendet.
8. In der Tabelle **Aktive Fehler** werden die Fehler für ein Gehäuse aufgeführt und angezeigt, die auf der Seite **Gehäusefunktionszustand** angezeigt werden. Für M1000e Version 4.3 und niedriger werden die aktiven Fehler nicht angezeigt.

Hardware-Bestandsliste anzeigen: Lüfter

Sie können Informationen über die Lüfter innerhalb des ausgewählten Gehäuses anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit Lüfterinformationen exportieren.

So zeigen Sie Informationen über Lüfter an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Um Informationen über die Lüfter anzuzeigen, führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf der Registerkarte **Übersicht** auf **Lüfter**.
   b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Lüfter**.

   Die folgenden Informationen werden angezeigt:

   - Name
   - Vorhanden
   - Stromzustand
   - Lesen
   - Warnungsschwelle
   - Kritischer Schwellenwert
     – Minimum
     – Maximal

Hardware-Bestandsliste anzeigen: E/A-Module

Sie können Informationen über die E/A-Module für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit Informationen zu E/A-Modulen exportieren.

So zeigen Sie Informationen über E/A-Module an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.

5. Um Informationen über die **E/A-Module** anzuzeigen, führen Sie einen der folgenden Schritte aus:

    a. Klicken Sie auf der Registerkarte **Übersicht** auf **E/A-Module**.

    b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **E/A-Module**.

    Die folgenden Informationen werden angezeigt:

    - Einschub/Standort
    - Vorhanden
    - Name
    - Struktur
    - Service-Tag-Nummer
    - Stromstatus

    Um zusätzliche Informationen anzuzeigen, wählen Sie das entsprechende E/A-Modul aus und die folgenden Informationen werden angezeigt:

    - Rolle
    - Firmware-Version
    - Hardwareversion
    - IP-Adresse
    - Subnetzmaske
    - Gateway
    - MAC-Adresse
    - DHCP aktiviert

Hardware-Bestandsliste anzeigen: iKVM

Sie können Informationen über das iKVM für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit iKVM-Informationen exportieren.



ANMERKUNG: Sie können Informationen über das iKVM-Modul nur für PowerEdge M1000e-Gehäuse anzeigen.

So zeigen Sie Informationen zum iKVM an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Um Informationen über das **iKVM** anzuzeigen, führen Sie einen der folgenden Schritte aus:

    a. Klicken Sie auf der Registerkarte **Übersicht** auf **iKVM**.

    b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **iKVM**.

    Die folgenden Informationen werden angezeigt:

- iKVM-Name
- Vorhanden
- Firmware-Version
- Frontblenden USB/Video aktiviert:
- Zugriff auf die CMC-CLI erlauben

ANMERKUNG: Die iKVM-Registerkarte wird nur dann angezeigt, wenn das Gehäuse ein iKVM-Modul enthält.

Hardware-Bestandsliste anzeigen: PCIe

Sie können Informationen über PCIe für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit PCIe-Informationen exportieren.

So zeigen Sie Informationen über PCIe an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Um Informationen über PCIe anzuzeigen, führen Sie einen der folgenden Schritte aus:

   ANMERKUNG: PCIe-Informationen sind nicht auf das M1000e-Gehäuse anwendbar.

   a. Klicken Sie auf der Registerkarte **Übersicht** auf **PCIe**.
   b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **PCIe**.

   Die folgenden Informationen werden angezeigt:

   - PCIe-Steckplatz
     – Steckplatz
     – Name
     – Stromstatus
     – Struktur
   - Serversteckplatz
     – Name
     – Nummer

   Um zusätzliche Informationen anzuzeigen, wählen Sie das entsprechende PCIe-Element aus und die folgenden Informationen werden angezeigt:

   - Steckplatztyp
   - Server-Zuordnung
   - Zuweisungsstatus
   - Zugewiesener Steckplatzstrom
   - PCI-ID

- Hersteller-ID

Hardware-Bestandsliste anzeigen: Netzteile

Sie können Informationen über die Netzteile für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit Informationen zu Netzteilen exportieren.

So zeigen Sie Informationen über das Netzteil an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Um Informationen zu den Netzteilen anzuzeigen, führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf der Registerkarte **Übersicht**auf **Netzteile**.

   b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Netzteile**.

   Die folgenden Informationen werden angezeigt:

   - Name
   - Kapazität
   - Vorhanden
   - Stromzustand

Hardware-Bestandsliste anzeigen: Temperatursensoren

Sie können Informationen über Temperatursensoren für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit Informationen zu Temperatursensoren exportieren.

So zeigen Sie Informationen über die Temperatursensoren an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Um Informationen über die Temperatursensoren anzuzeigen, führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf der Registerkarte **Übersicht** auf **Temperatursensoren**.

   b. Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Temperatursensoren**.

   Die folgenden Informationen werden angezeigt:

   - Standort
   - Reading

- Warnungsschwelle
  - Minimum
  - Maximal
- Kritischer Schwellenwert
  - Minimum
  - Maximal

 **ANMERKUNG:** Für PowerEdge M1000e-Gehäuse werden Informationen über Temperatursensoren nur für Gehäuse angezeigt. Für andere Gehäuse werden Informationen über Temperatursensoren für Gehäuse und zugeordnete modulare Server angezeigt.

Anzeigen von Einzelheiten der Garantie

Im Garantiefenster werden die Einzelheiten zur Garantie gespeichert.

So zeigen Sie Informationen über die Garantie an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Die Registerkarte **Garantie** enthält Folgendes:
   a. **Anbieter**
   b. **Beschreibung**
   c. **Status**
   d. **Startdatum**
   e. **Enddatum**
   f. **Verbleibende Tage**
   g. **Zuletzt aktualisiert**

Anzeigen des Speichers

Im Speicher-Fenster werden die Informationen für das Gehäuse gespeichert.

So zeigen Sie Informationen über den Speicher an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Die Registerkarte **Speicher** enthält folgendes:
   a. **Virtuelle Festplatten**
   b. **Controller**
   c. **Gehäuse**

   d. **Physische Festplatten**
   e. **Ersatzlaufwerke**

   Wenn Sie auf einen einzelnen markierten Link unter „Speicher“ klicken, zeigt die Tabelle **Ansicht** die Details für jedes markierte Objekt. Wenn Sie in der Ansichts-Tabelle auf jedes Zeilenobjekt klicken, werden zusätzliche Informationen für jedes markierten Objekt angezeigt.

6. Wenn Sie bei M1000e-Gehäusen ein Speicher-Modul besitzen, werden die folgenden Speicher-Details in einer Rasteransicht ohne zusätzliche Informationen angezeigt.
   a. Name
   b. Modell
   c. Service-Tag-Nummer
   d. IP-Adresse (Link zum Speicher)
   e. Struktur
   f. Gruppenname
   g. Gruppen-IP-Adresse (Link zur Speichergruppe)

Anzeigen von Firmware-Details für ein Gehäuse

Sie können Informationen über die Firmware-Details für das ausgewählte Gehäuse anzeigen. Sie können eine CSV-Datei mit Firmware-Informationen exportieren.

So zeigen Sie Informationen über die Firmware an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Klicken Sie auf die Doppelpfeil-Markierung, erweitern Sie den linken Fensterbereich und klicken Sie anschließend auf **Firmware**.

   Die folgenden Informationen werden angezeigt:

   - Komponente
   - Aktuelle Version
6. Wenn Sie auf die Schaltfläche **CMC starten** klicken, wird die Seite **Chassis Management Controller** angezeigt.

Anzeigen von Management-Controller-Details für ein Gehäuse

Sie können Informationen über die Details des Management Controllers für das ausgewählte Gehäuse anzeigen.

So zeigen Sie Informationen über den Management Controller an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Überwachen**.
5. Klicken Sie auf die Doppelpfeil-Markierung, erweitern Sie den linken Fensterbereich und klicken Sie anschließend auf **Firmware**.
6. Um zusätzliche Informationen anzuzeigen, klicken Sie auf der Seite **Management Controller** auf die Pfeilmarkierung und erweitern Sie die linke Spalte.

   Die folgenden Informationen werden angezeigt:

- Allgemein
  - Name
  - Firmware-Version
  - Zeitpunkt der letzten Aktualisierung
  - CMC-Standort
  - Hardwareversion
- Gemeinsames Netzwerk
  - DNS-Domänenname
  - DHCP für DNS verwenden
  - MAC-Adresse
  - Redundanzmodus
- CMC-IPv4-Informationen
  - IPv4 aktiviert
  - DHCP aktiviert
  - IP-Adresse
  - Subnetzmaske
  - Gateway
  - Bevorzugter DNS-Server
  - Alternativer DNS-Server

Anzeigen des zugeordneten Hosts für ein Gehäuse

Sie können Informationen über die zugeordneten Hosts für das ausgewählte Gehäuses auf der Seite **Verwalten** anzeigen.

So zeigen Sie Informationen zu dem zugeordneten Host an:

1. Klicken Sie auf der **Startseite** auf **vCenter Server**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Verwalten**.

   Die folgenden Informationen über den zugeordneten Host werden angezeigt:

   - Host-Name (Falls Sie auf die ausgewählten Host-IP-Adresse klicken, werden die Details zum Host angezeigt.)
   - Service-Tag-Nummer
   - Modell
   - iDRAC IP (iDRAC-IP)
   - Einschubposition
   - Letzte Bestandsaufnahme

13

Überwachung eines einzigen Hosts

Die OpenManage Integration for VMware vCenter ermöglicht Ihnen die Anzeige detaillierter Informationen für einen einzelnen Host. Sie können vom Navigator auf der linken Seite her auf Hosts in VMware vCenter zugreifen. Dadurch werden alle Hosts für alle Anbieter angezeigt. Klicken Sie auf einen spezifischen Dell-Host, um detailliertere Informationen yu finden. Um schnell eine Liste von Dell-Hosts anzuzeigen, klicken Sie von innerhalb der OpenManage Integration for VMware vCenter im linken Navigator auf Dell-Hosts.

- Hostzusammenfassungsdetails anzeigen
- Anzeigen der Hardware: FRU-Details für einen einzigen Host
- Anzeigen der Hardware: Prozessordetails für einen einzigen Host
- Anzeigen der Hardware: Netzteildetails für einen einzigen Host
- Anzeigen der Hardware: Speicherdetails für einen einzigen Host
- Anzeigen der Hardware: NICs-Details für einen einzigen Host
- Anzeigen der Hardware: PCI-Steckplatzdetails für einen einzigen Host
- Anzeigen der Hardware: Details der Remote-Zugriffskarten für einen einzigen Host
- Speicherdetails für einen einzigen Host anzeigen
  - Speicher anzeigen: Details der virtuellen Festplatte für einen einzigen Host
  - Speicher anzeigen: Details der physischen Festplatte für einen einzigen Host
  - Speicher anzeigen: Controllerdetails für einen einzigen Host
  - Speicher anzeigen: Gehäusedetails für einen einzigen Host
- Firmwaredetails für einen einzigen Host anzeigen
- Stromüberwachung für einen einzigen Host anzeigen
- Garantiestatus für einen einzigen Host anzeigen
- Nur Dell-Hosts schnell anzeigen

Hostzusammenfassungsdetails anzeigen

Zeigen Sie die Hostzusammenfassungsdetails für einen individuellen Host auf der Seite Hostzusammenfassung an. Diese Seite zeigt verschiedene Portlets an. Zwei dieser Portlets sind für die OpenManage Integration for VMware vCenter gültig.

Die Portlets sind:

- Dell Host-Funktionszustand
- Dell Host-Informationen

Sie können diese Portlets auf die gewünschte Position ziehen und ablegen, und Sie können die zwei Portlets wie andere Portlets entsprechend Ihren Anforderungen formatieren und anpassen.

1. Klicken Sie inOpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie auf der Registerkarte „Objekte" einen spezifischen Host aus, den Sie überprüfen wollen.
3. Klicken Sie auf die Registerkarte **Zusammenfassung**.
4. Zeigen Sie die Hostzusammenfassungsdetails an:

Alarmsystem Wenn Alarme für dieOpenManage Integration for VMware vCenter vorhanden sind, werden diese unterhalb des Statusbereiches und oberhalb der Portlets in einem gelben Kästchen angezeigt.

Benachrichtigungsbereich Dell Produkte integrieren Informationen in dieses Feld auf der rechten Seite. Hier finden Sie folgende Informationen:

- Letzte Tasks
- In Bearbeitung
- Alarme
  Dell-Alarminformationen werden in diesem Benachrichtigungsbereich-Portlet angezeigt.

5. Führen Sie zur Anzeige des Dell Server Management-Portlets einen Bildlauf nach unten durch.

Service-Tag-Nummer Die Service-Tag-Nummer Ihres Dell PowerEdge Servers. Verwenden Sie diese Nummer, wenn Sie den Support anrufen.

Modellname Zeigt den Modellnamen des Servers an.

Fault Resilient Memory Dies ist ein BIOS-Attribut und wird während dem ersten Einrichten des Servers im BIOS aktiviert und zeigt den Speicherbetriebsmodus auf dem Server an. Sie müssen Ihr System neu starten, wenn Sie die Speicherbetriebsmodus-Werte ändern. Dies gilt für R620-, R720-, T620-, M620-Server mit ESXi 5.5-Version oder höher. Dies gilt für Server der 12. Generation von PowerEdge-Servern und später, die die Option 'Fehlerbeständiger Speicher' unterstützt und auf denen ESXi 5.5 oder später ausgeführt wird. Dies gilt auch für Server der 13. Generation. Die vier verschiedenen Werte sind:

- Aktiviert und geschützt: Dieser Wert bedeutet, dass das System unterstützt wird und das Betriebssystem-Version ESXi 5.5 oder höher ist sowie, dass der Speicherbetriebsmodus in BIOS auf FRM eingestellt ist.
- Aktiviert und nicht geschützt: Dieser Wert zeigt an, dass Systeme mit Betriebssystem-Versionen niedriger als ESXi 5.5 unterstützt werden.
- Deaktiviert: Dieser Wert zeigt an, dass gültige Systeme mit jeglichen Betriebssystem-Versionen unterstützt werden und der Speicherbetriebsmodus in BIOS nicht auf FRM gesetzt ist.
- Leer: Wenn der Speicherbetriebsmodus in BIOS nicht unterstützt wird, wird das FRM-Attribut nicht angezeigt.

Identifikation

- Host-Name
  Der Name Ihres Dell-Hosts.
- Stromzustand
  Zeigt an, ob der Strom eingeschaltet oder aus ist.
- iDRAC IP (iDRAC-IP)

	Zeigt die IP-Adresse des iDRACs an. • Verwaltungs-IP Zeigt die Verwaltungs-IP-Adresse an. • Verbindungsprofil Zeigt den Verbindungsprofilname für diesen Host an. • Modell Zeigt das Dell Server-Modell an. • Service-Tag-Nummer Zeigt die Service-Tag-Nummer des Servers an. • Systemkennnummer Zeigt die Systemkennnummer an. • Verbleibende Garantiezeit in Tagen Zeigt die verbleibende Garantiezeit in Tagen an. • Letzter Bestandsaufnahme-Scan Zeigt das Datum und die Uhrzeit des letzten Bestandsaufnahme-Jobs an.
Hypervisor und Firmware	• Hypervisor Zeigt die Hypervisor-Version an. • BIOS-Version Zeigt die BIOS-Version an. • Version der Remote-Zugriffskarte Zeigt die Version der Remote-Zugriffskarte an.
Management-Konsolen	Die Management-Konsolen dienen zum Starten der externen System Management-Konsolen. Dazu gehören: • Remote-Zugriffskonsole (iDRAC) Startet die Web-Benutzeroberfläche des iDRAC (Integrated Dell Remote Access Controller).
Hostmaßnahmen	Blinkanzeigelicht ermöglicht es Ihnen den Server so einzurichten, dass er in verschiedenen Zeitintervallen blinkt.

6. Anzeigen des Dell Host-Funktionszustands-Portlets:

Dell Host-Funktionszustand	Der Funktionszustand einer Komponente ist eine grafische Darstellung des Status aller wichtigen Host-Server-Komponenten: globaler Status des Servers, Server, Netzteile, Temperaturen, Spannungen, Prozessoren, Batterien, Eingriff, Hardware-Protokoll, Energieverwaltung, Leistung und Speicher. Die Gehäusefunktionszustandsparameter gelten für die Modelle **VRTX Version 1.0 und höher**, **M1000e Version 4.4 und höher**. Für Versionen unter 4.3 werden nur zwei Anzeigen für den Funktionszustand angezeigt: **Funktionsfähig** und **Warnung oder Kritisch** (Umgekehrtes Dreieck mit einem Ausrufezeichen in orangener Farbe). Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit dem niedrigsten Funktionszustandsparameter an. Wenn zum Beispiel 5 Zeichen für funktionsfähig und 1 Warnzeichen angezeigt werden, wird der Gesamtfunktionszustand als Warnung angezeigt. Zu den Optionen gehören: • Funktionsfähig (grünes Häkchen) – Komponente arbeitet normal • Warnung (gelbes Dreieck mit Ausrufezeichen) – Komponente weist einen nichtkritischen Fehler auf

- Kritisch (rotes X) – Komponente weist einen kritischen Fehler auf
- Unbekannt (Fragezeichen) – der Status der Komponente ist unbekannt

Starten von Verwaltungskonsolen

Sie können zwei Verwaltungskonsolen vom Dell Server Management Portlet aus starten. Diese sind:

- Remote-Zugriffskonsole (iDRAC-Konsole)
  Starten Sie die Remote-Zugriffskonsole, um auf die iDRAC-Benutzerschnittstelle zuzugreifen.
- OMSA-Konsole.
  Starten Sie die OMSA-Konsole, um die OpenManage Server Administrator-Schnittstelle aufzurufen. Vor dem Starten der OMSA-Konsole muss die OMSA-URL in der Open Management Integration konfiguriert werden.

Starten der Remote-Zugriffskonsole (iDRAC)

Sie können die iDRAC-Benutzeroberfläche vom Dell Server Management Portlet aus starten.

1. Klicken Sie im Navigator-Bereich des OpenManage Integration for VMware vCenter unter Bestandslisten auf **Hosts**.
2. Doppelklicken Sie auf der Registerkarte „Objekt" auf den gewünschten Host.
3. Führen Sie auf der Registerkarte „Zusammenfassung" einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Klicken Sie auf **Management-Konsolen** → **Remote-Zugriffskonsole (iDRAC)**.

Starten der OMSA-Konsole

Bevor Sie die OMSA-Konsole starten, müssen Sie die OMSA-URL einrichten und den OMSA-Web Server installieren und konfigurieren. Richten Sie die OMSA-URL von dem Register „Einstellungen" aus ein.



ANMERKUNG: Sie müssen OMSA installieren, um Dell PowerEdge-Server der 11. Generation unter Verwendung des OpenManage Integration for VMware vCenter zu überwachen und verwalten.

1. Klicken Sie im Navigator-Bereich des OpenManage Integration for VMware vCenter unter Bestandsaufnahmelisten auf **Hosts**.
2. Doppelklicken Sie im Register „Objekt" auf den gewünschten Host.
3. Führen Sie im Register „Zusammenfassung" einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Klicken Sie zum Öffnen der OMSA-Konsole auf **Verwaltungskonsolen** → **OMSA-Konsole**.

Starten der Remote-Zugriffskonsole (iDRAC)

Sie können die iDRAC-Benutzeroberfläche vom Dell Server Management Portlet aus starten.

1. Klicken Sie im Navigator-Bereich des OpenManage Integration for VMware vCenter unter Bestandslisten auf **Hosts**.
2. Doppelklicken Sie auf der Registerkarte „Objekt" auf den gewünschten Host.
3. Führen Sie auf der Registerkarte „Zusammenfassung" einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Klicken Sie auf **Management-Konsolen** → **Remote-Zugriffskonsole (iDRAC)**.

Einrichten eines Blinkanzeigelichts an der Frontblende eines physischen Servers

Sie können ein Anzeigelicht an der Frontblende eines physischen Servers in einer großen Datacenter-Umgebung über einen bestimmten Zeitraum blinken lassen, so dass Sie den Server leichter erkennen können.

1. Klicken Sie imOpenManage Integration for VMware vCenter im Navigationsbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie auf der Registerkarte „Objekt“ auf den gewünschten Host.
3. Führen Sie auf der Registerkarte „Zusammenfassung“ einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Wählen Sie unter **Hostaktionen** die Option **Blinkanzeigelicht**.
5. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie zum Einschalten des Blinkens und zum Einrichten einer Dauer im Dialogfeld **Anzeigelicht** auf **Blinken eingeschaltet**, und wählen Sie in der Dropdown-Liste „Zeitüberschreitung“ eine Dauer aus, dann klicken Sie auf **OK**.
   - Klicken Sie zum Ausschalten des Blinkens im Dialogfeld **Anzeigelicht** auf **Blinken ausgeschaltet** und dann auf **OK**.

Einrichten eines Blinkanzeigelichts an der Frontblende eines physischen Servers

Sie können ein Anzeigelicht an der Frontblende eines physischen Servers in einer großen Datacenter-Umgebung über einen bestimmten Zeitraum blinken lassen, so dass Sie den Server leichter erkennen können.

1. Klicken Sie imOpenManage Integration for VMware vCenter im Navigationsbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie auf der Registerkarte „Objekt“ auf den gewünschten Host.
3. Führen Sie auf der Registerkarte „Zusammenfassung“ einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Wählen Sie unter **Hostaktionen** die Option **Blinkanzeigelicht**.
5. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie zum Einschalten des Blinkens und zum Einrichten einer Dauer im Dialogfeld **Anzeigelicht** auf **Blinken eingeschaltet**, und wählen Sie in der Dropdown-Liste „Zeitüberschreitung“ eine Dauer aus, dann klicken Sie auf **OK**.
   - Klicken Sie zum Ausschalten des Blinkens im Dialogfeld **Anzeigelicht** auf **Blinken ausgeschaltet** und dann auf **OK**.

14

Erwerb und Hochladen einer Software-Lizenz

Bis zum Upgrade (zur Erweiterung) auf eine volle Produktversion führen Sie eine Testversion aus. Verwenden Sie den Link *Lizenz kaufen* des Produkts, um zur Dell Website zu navigieren und eine Lizenz zu erwerben. Laden Sie diese nach dem Kauf unter Verwendung der Verwaltungskonsole hoch. Diese Option wird nur angezeigt, wenn Sie eine Testlizenz verwenden.

1. Führen Sie in OpenManage Integration for VMware vCenter einen der folgenden Schritte aus:

   - Klicken Sie im Register **Lizenzierung** neben „Software Lizenz" auf **Lizenz kaufen**.
   - Klicken Sie im Register „Zum Einstieg" unter „grundlegende Tasks" auf **Lizenz kaufen**.

   ANMERKUNG: Die Lizenz wird per E-Mail als XML-Datei versandt. Lizenzierungsfragen senden Sie mit der ursprünglichen Bestellnummer in einer E-Mail an **download_software@dell.com**.
2. Kaufen Sie Ihre Lizenz auf der Dell-Webseite und speichern Sie die Datei auf einem bekannten Speicherort.
3. Geben Sie die Verwaltungskonsolen-URL in einen Web-Browser ein.

   Verwenden Sie dieses Format: https://<GeräteIPAdresse>
4. Geben Sie im Anmeldefenster der Verwaltungskonsole das Kennwort ein und klicken Sie auf **Anmelden**.
5. Klicken Sie auf Lizenz **hochladen**.
6. Klicken Sie zum Suchen der Lizenzdatei im Fenster „Lizenz hochladen" auf **Durchsuchen**.
7. Wählen Sie die Lizenzdatei aus und klicken Sie auf **Hochladen**.

Informationen über die OpenManage Integration for VMware vCenter-Lizenzierung

Die OpenManage Integration for VMware vCenter verfügt über zwei Arten von Lizenzen:

Test-Lizenz	Die Test-Lizenz beinhaltet eine Demo-Lizenz für fünf Hosts (Server), die durch OpenManage Integration for VMware vCenter verwaltet werden. Dies gilt nur für die 11. und höhere Generationen. Dies ist eine Standardlizenz und gilt für einen Zeitraum von 90 Tagen.
Produkt-Lizenz	Die Produkt-Vollversion enthält eine Standardlizenz für bis zu zehn vCenter und die erworbene Anzahl an Hostverbindungen, die vom OpenManage Integration for VMware vCenterverwaltet werden.

Wenn Sie von einer Test-Lizenz zu einer Produkt-Lizenz erweitern, wird Ihnen eine neue XML-Datei per E-Mail zugesendet. Speichern Sie die Datei auf Ihrem lokalen System und laden Sie die neue Lizenzdatei unter Verwendung der Administration Console hoch. Die Lizenzierung zeigt die folgenden Informationen an:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu zehn registrierte und verwendete vCenter-Verbindungen sind zulässig.
- Höchstzahl der Host-Verbindungslizenzen – die Anzahl an erworbenen Lizenzen für Hostverbindungen.
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern) die erfasst und in die Bestandsliste aufgenommen wurden.

- Verfügbar – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.

 ANMERKUNG: Der Standardlizenzzeitraum beträgt nur 3 Jahre und die zusätzlichen Lizenzen werden der vorhandenen Lizenz beigefügt und nicht überschrieben. Sie können die 9. und 10. Generation nicht einem neuen oder vorhandenen Profil hinzufügen, wenn die Gesamtanzahl von Hosts der 11., 12. und 13. Generation, für welche die Bestandsaufnahme erfolgreich durchgeführt wurde, die Sperrnummer erreicht hat.

15

Anzeigen der Hardware: FRU-Details für einen einzigen Host

Zeigen Sie die Details für die Austauschbare Funktionseinheit(FRU) für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie die Hardware: FRU-Details anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Informationen** aus und lassen Sie im Unterregister „Hardware: FRU“ Folgendes anzeigen:

Teilename	Zeigt den Teilenamen der FRU an
Teilenummer	Zeigt die Teilenummer der FRU an.
Hersteller	Zeigt den Herstellernamen an.
Seriennummer	Zeigt die Hersteller-Seriennummer an.
Manufacture Date	Zeigt das Herstellungsdatum an.

16 Anzeigen der Hardware: Prozessordetails für einen einzigen Host

Zeigen Sie die Prozessordetails für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie die Prozessordetails anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Informationen** aus und lassen Sie im Unterregister „Hardware: Prozessor“ Folgendes anzeigen:

Sockel	Zeigt die Steckplatznummer an.
Geschwindigkeit	Zeigt die aktuelle Geschwindigkeit an.
Marke	Zeigt die Prozessormarke an.
Version	Zeigt die Prozessorversion an.
Kerne	Zeigt die Anzahl der Prozessorkerne an.

17 Anzeigen der Hardware: Netzteildetails für einen einzigen Host

Zeigen Sie die Netzteildetails für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie die Hardware: Netzteildetails anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Hardware: Netzteil** Folgendes anzeigen:

Typ — Zeigt den Netzteiltyp an. Die Netzteiltypen beinhalten folgendes:

- UNBEKANNT
- LINEAR
- SCHALTNETZTEIL
- BATTERY
- USV
- UMWANDLER
- REGULATOR
- Wechselstrom (AC)
- Gleichstrom (DC)
- VRM

Standort — Zeigt den Standort des Netzteils an, z.B. Steckplatz 1.

Ausgabe (Watt) — Zeigt die Stromkapazität in Watt an.

18

Anzeigen der Hardware: Speicherdetails für einen einzigen Host

Zeigen Sie die Speicher-Details für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte" einen spezifischen Host aus, für den Sie die Hardware: Speicher-Details anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen" das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Hardware: Speicher** Folgendes anzeigen:

Speichersteckplätze	Zeigt die verwendete, gesamte und verfügbare Speicheranzahl an.
Speicherkapazität	Zeigt die installierten Speicher, Gesamtspeicherkapazität und verfügbaren Speicher an.
Steckplatz	Zeigt den DIMM-Steckplatz an.
Größe	Zeigt die Speichergröße an.
Typ	Zeigt den Speichertyp an.

19 Anzeigen der Hardware: NICs-Details für einen einzigen Host

Zeigen Sie die Network Interface Card (NIC)-Details für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie Hardware: NICs-Details anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Hardware: NICs** Folgendes anzeigen:

Gesamt	Zeigt die Gesamtanzahl der verfügbaren Netzwerkschnittstellenkarten an.
Name	Zeigt den NIC-Namen an.
Hersteller	Zeigt nur den Herstellernamen an.
MAC-Adresse	Zeigt die MAC-Adresse der NIC an.

20

Anzeigen der Hardware: PCI-Steckplätze für einen einzigen Host

Zeigen Sie die PCI-Steckplatzdetails für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im Navigator des OpenManage Integration for VMware vCenter auf **Hosts**.
2. Wählen Sie im Register „Objekte" einen spezifischen Host aus, für den Sie die Hardware: PCI-Steckplatzdetails anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen" das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Hardware: PCI-Steckplätze** Folgendes anzeigen:

PCI-Steckplätze	Zeigt die verwendeten, gesamten und verfügbaren PCI-Steckplätze an.
Steckplatz	Zeigt den Steckplatz an.
Hersteller	Zeigt den Herstellernamen des PCI-Steckplatzes an.
Beschreibung	Zeigt die Beschreibung des PCI-Geräts an.
Typ	Zeigt den Typ des PCI-Steckplatzes an.
Breite	Zeigt die Datenbusbreite an, wenn verfügbar.

21

Anzeigen der Hardware: Details der Remote-Zugriffskarten für einen einzigen Host

Zeigen Sie die Details der Remote-Zugriffskarten für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im Navigator OpenManage Integration for VMware vCenter auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie die Details der Remote-Zugriffskarten anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Hardware: Remote-Zugriffskarte** Folgendes anzeigen:

IP-Adresse	Zeigt die IP-Adresse der Remote-Zugriffskarte an.
MAC-Adresse	Zeigt die MAC-Adresse der Remote-Zugriffskarte an.
RAC-Typ	Zeigt den Typ der Remote-Zugriffskarte an.
URL	Zeigt die verfügbare URL für den iDRAC an, der diesem Host zugeordnet wurde.

22

Speicherdetails für einen einzigen Host anzeigen

Zeigen Sie die Speicherdetails für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs. Diese Seite zeigt verschiedene Optionen an, abhängig von der Auswahl aus der Drop-Down-Liste „Ansicht". Wenn Sie „Physische Festplatten" auswählen, erscheint eine neue Drop-Down-Liste. Diese neue Drop-Down-Liste, Filter genannt, ermöglicht es Ihnen, Ihre physischen Optionen zu filtern.



ANMERKUNG: Hardwareansichten melden die Daten aus OMSA und iDRAC direkt.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte" einen spezifischen Host aus, für den Sie die „Speicher: Details zur physischen Festplatte" anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen" das Register **Dell Host Informationen** aus und lassen Sie im Unterregister **Speicher** Folgendes anzeigen:

Bei Lagerung	Zeigt die Anzahl der virtuellen Festplatten, Controller, Gehäuse und zugehörige physische Festplatten mit der Anzahl ihrer Globalen Hotspares und Dedizierten Hotspares an. Wenn Sie eine Option aus der Drop-Down-Liste „Ansicht" ausgewählt haben, wird die Auswahl hier hervorgehoben.
Ansicht	Zeigt die Seiten-Optionen an, die Sie für diesen Host anzeigen möchten. • Virtuelle Festplatten • Physische Festplatten • Controller • Gehäuse

Anzeigen der Hardware: Details der virtuellen Festplatte für einen einzigen Host

Die Speicheroptionen auf der Seite Host-Speicher hängen davon ab, was Sie aus der Drop-Down-Liste auswählen.

Wenn Sie „Virtuelle Festplatte" aus der Drop-Down-Liste ausgewählt haben, zeigen Sie diese Optionen an:

Name	Zeigt den Namen der virtuellen Festplatte an.
Geräte-FQDD	Zeigt die FQDD an.
Physische Festplatte	Zeigt an, auf welcher physischen Festplatte sich die virtuelle Festplatte befindet.
Kapazität	Zeigt die Kapazität der virtuellen Festplatte an.
Layout	Zeigt den Layout-Typ des virtuellen Speichers an. Damit ist der für diese virtuelle Festplatte konfigurierte RAID-Typ gemeint.

Datenträgertyp	Zeigt entweder SSD oder HDD an.
Controller ID	Anzeige der Controller-ID.
Geräte-ID	Anzeige der Geräte-ID.
Stripe-Größe	Die Stripe-Größe bezieht sich auf die Menge an Speicherplatz, die jeder Stripe auf einer einzelnen Festplatte belegt.
Busprotokoll	Dies zeigt die von den in der virtuellen Festplatte enthaltenen physischen Festplatten verwendete Technologie an. Mögliche Werte sind: • SCSI • SAS • SATA
Standard-Leserichtlinie	Die durch den Controller standardmäßig unterstützte Leserichtlinie. Die Optionen beinhalten: • Vorauslesen • Kein Vorauslesen • Adaptives Vorauslesen • Lese-Cache aktiviert • Lese-Cache deaktiviert
Standard-Schreibrichtlinie	Die durch den Controller standardmäßig unterstützte Schreibrichtlinie. Die Optionen beinhalten: • Rückschreiben • Rückschreiben erzwingen • Rückschreiben aktiviert • Durchschreiben • Schreib-Cache aktiviert und geschützt. • Schreib-Cache deaktiviert
Cache-Regeln	Wird angezeigt, wenn die Cache-Regeln aktiviert sind.

Speicher anzeigen: Details der physischen Festplatte für einen einzigen Host

Die Speicheroptionen auf der Seite Host-Speicher hängen davon ab, was Sie aus der Drop-Down-Liste auswählen. Wenn Sie diese Option auswählen, wird die Drop-Down-Liste „Filter“ angezeigt. Sie können Ihre physische Festplatte durch die folgenden Optionen filtern:

- Alle physischen Festplatten
- Globale Hotspares
- Dedizierte Ersatzgeräte
- Diese Option wird angezeigt, wenn Sie virtuelle Laufwerke mit eigenen Namen erstellt haben.

Wenn Sie aus der Drop-Down-Liste „Physische Festplatten“ ausgewählt haben, werden diese Optionen angezeigt:

Name	Zeigt den Namen des physischen Laufwerks an.
Geräte-FQDD	Zeigt die Geräte-FQDD an.
Kapazität	Zeigt die Kapazität der physischen Festplatte an.
Festplattenstatus	Zeigt den Status der physischen Festplatte an. Die Optionen beinhalten folgendes: • ONLINE • BEREIT • HERABGESETZT • FEHLGESCHLAGEN • OFFLINE • NEUERSTELLUNG • INKOMPATIBEL • ENTFERNT • GELÖSCHT • SMART-WARNUNG FESTGESTELLT • UNBEKANNT • FREMD • NICHT UNTERSTÜTZT
Konfiguriert	Zeigt an, ob die Festplatte konfiguriert ist.
Hotspare-Typ	Zeigt den Hot-Spare-Typ an. Die Optionen beinhalten folgendes: • Nein Nein bedeutet, dass kein Hot-Spare vorhanden ist. • Global Ein globales Hot-Spare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist. • Dediziert Ein dedizierter Hotspare ist eine nicht verwendete Backup-Festplatte, die einer einzelnen virtuellen Festplatte zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte versagt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen.
Virtuelle Festplatte	Zeigt den Namen der virtuellen Festplatte an.
Busprotokoll	Zeigt das Bus-Protokoll an.
Controller ID	Anzeige der Controller-ID.
Konnektor-ID	Zeigt die Konnektor-ID an.
Gehäuse-ID	Zeigt die Gehäuse-ID an.
Geräte-ID	Anzeige der Geräte-ID.
Modell	Zeigt die Modellnummer des physischen Speichergeräts an.
Teilenummer	Zeigt die Speicherteilenummer an.
Seriennummer	Zeigt die Speicherseriennummer an.

Hersteller	Zeigt den Speicheranbieternamen an.

Speicher anzeigen: Controllerdetails für einen einzigen Host

Die Speicheroptionen auf der Seite Host-Speicher hängen davon ab, was Sie aus der Drop-Down-Liste auswählen.

Wenn Sie „Controller“ aus der Drop-Down-Liste „Ansicht“ ausgewählt haben, zeigen Sie diese Optionen an:

Controller ID	Anzeige der Controller-ID.
Name	Zeigt den Namen des Controllers an.
Geräte-FQDD	Zeigt die FQDD des Geräts an.
Firmware-Version	Anzeige der Firmware-Version.
Mindestens erforderliche Firmware	Zeigt die mindestens erforderliche Firmware an. Diese Spalte wird automatisch befüllt, wenn die Firmware veraltet ist und eine neuere Version verfügbar ist.
Treiberversion	Zeigt die Treiberversion an.
Patrol Read-Zustand	Zeigt den Patrol Read-Zustand an.
Cache-Größe	Zeigt die Größe des Caches an.

Speicher anzeigen: Gehäusedetails für einen einzigen Host

Die Speicheroptionen auf der Seite Host-Speicher hängen davon ab, was Sie aus der Drop-Down-Liste auswählen.

Wenn Sie „Gehäuse“ aus der Drop-Down-Liste ausgewählt haben, zeigen Sie diese Optionen an:

Controller ID	Anzeige der Controller-ID.
Konnektor-ID	Zeigt die Konnektor-ID an.
Gehäuse-ID	Zeigt die Gehäuse-ID an.
Name	Zeigt den Namen des Gehäuses an.
Geräte-FQDD	Zeigt die Geräte-FQDD an.
Service Tag	Zeigt die Service-Tag-Nummer an.

23 Anzeigen von Firmwaredetails für einen einzigen Host

Zeigen Sie die Firmwaredetails für einen einzigen Host im Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs. Diese Host-Seite ermöglicht es Ihnen, die Suchfilter zu verwenden und eine CSV-Datei von Firmware-Informationen zu exportieren.

1. Klicken Sie im Navigator des OpenManage Integration for VMware vCenter auf **Hosts**.
2. Wählen Sie im Register „Objekte" einen spezifischen Host aus, für den Sie die Firmware-Details anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen" das Register **Dell Host Informationen** aus und lassen Sie im Unterregister „Firmware" Folgendes anzeigen:

Name	Zeigt den Namen von sämtlicher Firmware auf diesem Host an.
Typ	Zeigt den Firmware-Typ an.
Version	Zeigt die Version von sämtlicher Firmware auf diesem Host an.
Installationsdatum	Zeigt das Installationsdatum an.

24

Stromüberwachung für einen einzigen Host anzeigen

Zeigen Sie die Prozessordetails für einen einzigen Host auf dem Register Dell Host-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten aus OMSA und iDRAC direkt. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

 **ANMERKUNG:** Hostzeit, wie sie hier verwendet wird, bedeutet die Zeit des Orts, wo sich der Host befindet.

1. Klicken Sie im Navigator des OpenManage Integration for VMware vCenter auf **Hosts**.
2. Wählen Sie im Register „Objekte“ einen spezifischen Host aus, für den Sie die Details der Stromüberwachung anzeigen lassen wollen.
3. Wählen Sie im Register „Überwachen“ das Register **Dell Host Host-Informationen** aus und lassen Sie im Unterregister „Stromüberwachung“ Folgendes anzeigen:

Allgemeine Informationen	Zeigt das Strombudget und den aktuellen Profilnamen an.
Schwellenwert	Zeigt die Warnungs- und Fehlerschwellenwerte in Watt an.
Stromkapazitätsreserve	Zeigt die Unmittelbare- und Spitzenstromkapazitätsreserve in Watt an.
	Energiestatistiken
Typ:	Zeigt den Typ der Energiestatistiken an.
Startzeit der Messung (Hostzeit)	Zeigt das Datum und die Uhrzeit an, zu der der Host mit dem Energieverbrauch begonnen hat.
Endzeit der Messung (Hostzeit)	Zeigt das Datum und die Uhrzeit an, zu der der Energieverbrauch des Hosts gestoppt wurde.
Messwert	Dieser unmittelbare Wert ist der Durchschnittswert der Messwerte über einen Zeitraum von einer Minute
Typ:	Zeigt den Typ der Energiestatistiken an.
Startzeit der Messung (Hostzeit)	Zeigt das Datum und die Uhrzeit an, zu der die Spitzenleistung des Hosts begonnen hat.
Spitzenzeit (Host Time)	Zeigt das Datum und die Uhrzeit der Spitzen-Ampere des Hosts an.
Spitzenmesswert	Die Statistiken des Spitzenstroms des Systems bestehen aus dem Spitzenstromverbrauch des Systems (in Watt).

25

Garantiestatus für einen einzigen Host anzeigen

Sie müssen einen Garantie-Job ausgeführt haben, um einen Garantiestatus anzuzeigen. Siehe Sofortige Ausführung eines Garantie-Jobs.
Zeigt die Garantiestatusdetails für einen einzigen Host im Register Dell Host-Informationen an. Die Seite Garantiezusammenfassung ermöglicht es Ihnen, durch das Aktivieren oder Deaktivieren des Garantiezeitplans und das Einstellen der Mindesttageschwellenwertwarnung das Garantie-Verfallsdatum zu überwachen und Garantieeinstellungen zu kontrollieren, wenn Servergarantieinformationen von Dell-Online abgerufen werden. Siehe Garantieverlauf.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigator auf **Hosts**.
2. Wählen Sie im Register „Objekte" einen spezifischen Host aus, für den Sie die Details der Garantiezusammenfassung anzeigen lassen wollen.
3. Klicken Sie im Register „Überwachen" auf **Dell-Hostinformationen,** und dann auf das Unterregister **Garantie**. Es werden die folgenden Informationen angezeigt:

Anbieter	Zeigt den Namen des Anbieters der Garantie an.
Beschreibung	Zeigt eine Beschreibung an.
Startdatum	Zeigt das Startdatum der Garantie an.
Enddatum	Zeigt das Enddatum der Garantie an.
Verbleibende Tage	Zeigt die verbleibenden Tage für die Garantie an.
Letzte Aktualisierung	Zeigt das Datum der letzten Aktualisierung der Garantie an.

26

Schnellansicht von nur Dell-Hosts

Wenn Sie schnell nur Dell-Hosts ansehen möchten, können Sie dies von innerhalb der OpenManage Integration for VMware vCenter tun, und im Navigator können Sie Dell-Hosts auswählen.

1. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol OpenManage Integration.
2. Klicken Sie im Navigator unter OpenManage Integration for VMware vCenter auf Dell-Hosts.
3. Zeigen Sie auf der Registerkarte Dell-Host folgende Informationen an:

Host-Name	Zeigt einen Link an, der die IP-Adresse für jeden Dell-Host verwendet. Klicken Sie auf einen spezifischen Hostlink, um die Informationen des Dell-Hosts anzuzeigen.
vCenter	Zeigt die vCenter IP-Adresse für diesen Dell-Host an.
Cluster	Falls dieser Dell-Host sich in einem Cluster befindet, wird der Clustername hier angezeigt.
Verbindungsprofil	Zeigt den Namen des Verbindungsprofils an.

27

Überwachen von Hosts auf Clustern und Datacenters

Das OpenManage Integration for VMware vCenter ermöglicht es Ihnen, detaillierte Informationen für alle Hosts, die in einem Datacenter oder Cluster eingeschlossen sind, anzuzeigen. Mit diesen Seiten können Sie Daten durch Klicken auf den Zeilenkopf des Datengitters sortieren. Mit den Seiten Datacenter und Cluster können Sie Informationen in eine Datei importieren, und sie bieten Filter/- Such-Funktion auf dem Datengitter an. Details schließen Folgendes ein:

- Anzeigen von Host-Übersicht-Details
- Hardware anzeigen: FRUs
- Hardware anzeigen: Prozessordetails
- Hardware anzeigen: Netzteildetails
- Anzeigen von Hardware: Speicher-Details
- Hardware anzeigen: NICs
- Hardware anzeigen: PCI-Steckplatzdetails
- Hardware-Anzeige: Einzelheiten von Remote-Zugriffskarten
- Speicher anzeigen: Details einer physischen Festplatte
- Speicher anzeigen: Details einer virtuellen Festplatte
- Anzeige von Firmware-Details
- Anzeige der Stromüberwachung
- Anzeigen der Einzelheiten der Garantiezusammenfassung

28 Übersichtsdetails für Datacenter und Cluster

Zeigen Sie die Host-Details für Datacenter oder Cluster auf der Dell Datacenter/Cluster-Registerkarte an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Die angezeigten Daten können abhängig von der für den Datenzugriff gewählten Ansicht unterschiedlich ausfallen. Hardwareansichten melden die Daten aus OMSA und iDRAC direkt. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.



ANMERKUNG: Datacenter- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine CSV-Datei und stellen Filter-/Suchfunktionen im Datengitter bereit.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte" ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Host-Details anzeigen lassen wollen.
4. Wählen Sie auf der Registerkarte „Überwachen" das Register **Dell Datacenter/- Cluster-Informationen** → **Übersicht** aus, und zeigen Sie die Details an:

   ANMERKUNG: Wählen Sie zur Anzeige der vollständigen Detailliste einen spezifischen Host aus dem Datengitter aus.

   Datacenter-/ Cluster-Informationen
   Zeigt die folgenden Optionen an:
   - Datacenter-/Clustername
   - Die Anzahl der Dell-verwalteten Hosts
   - Gesamtenergieverbrauch
     Dieser Link führt Sie zur Seite Stromüberwachung für dieses Datacenter oder diesen Cluster.

   Hardware-Ressourcen
   Zeigt die folgenden Optionen an:
   - Gesamtanzahl der Prozessoren
     Dieser Link führt Sie zur Seite Prozessordetails .
   - Speicher insgesamt
     Dieser Link führt Sie zur Seite Speicherdetails für dieses Datacenter oder diesen Cluster.
   - Kapazität von virtuellen Laufwerken
     Dieser Link führt Sie zur Seite Virtuelle Festplatte für dieses Datacenter oder diesen Cluster.

   Garantiezusammenfassung
   Zeigt den Garantiestatus für den ausgewählten Host an. Die Statusoptionen beinhalten folgendes:
   - Abgelaufene Garantie
   - Aktive Garantie
   - Unbekannte Garantie

   Dieser Link führt Sie zur Seite Garantiezusammenfassung.

Host	Zeigt den Host-Namen an.
Service Tag	Zeigt die Service-Tag-Nummer des Hosts an.
Modell	Zeigt das Dell PowerEdge-Modell an.
Systemkennnummer	Zeigt die Systemkennnummer an, wenn konfiguriert.
Service-Tag-Nummer des Gehäuses	Zeigt die Gehäuse-Service-Tag-Nummer an, falls verfügbar.
Betriebssystemversion	Zeigt die ESXi oder ESX OS-Version an.
Standort	Nur Blades: Standort zeigt die Einschubposition an. Sonst zeigt der Standort „Nicht zutreffend“ an.
iDRAC IP (iDRAC-IP)	Zeigt die IP-Adresse des iDRACs an.
Service-Konsolen-IP	Zeigt die Service-Konsolen-IP an.
CMC URL	Nur Blades: Die CMC URL zeigt die Gehäuse-URL an. Sonst zeigt sie „Nicht zutreffend“ an.
CPUs	Zeigt die Anzahl der CPUs an.
Speicher	Zeigt den Host-Speicher an.
Stromzustand	Zeigt an, ob der Host mit Strom versorgt wird.
Letzte Bestandsaufnahme	Zeigt den Tag, das Datum und die Uhrzeit des letzten Bestandsaufnahme-Jobs an.
Verbindungsprofil	Zeigt den Namen des Verbindungsprofils an.
Version der Remote-Zugriffskarte	Zeigt die Version der Remote-Zugriffskarte an.
BIOS-Firmware-Version	Zeigt die Firmware-Version des BIOS an.

29

Anzeigen der Hardware: FRUs für Datacenter oder Cluster

Zeigen Sie die Details für Austauschbare Funktionseinheit (FRU) für ein Datacenter oder Cluster auf der Registerkarte Dell Datacenter/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Mit Datacenter- und Clusterseiten können Sie Informationen in eine CSV-Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Die angezeigten Daten können abhängig von der für den Datenzugriff gewählten Ansicht unterschiedlich ausfallen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ einen spezifischen Host, Datacenter oder Cluster aus, für den Sie die Hardware-FRU-Details anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: FRU** Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Teilename	Zeigt den Teilenamen der FRU an
Teilenummer	Zeigt die Teilenummer der FRU an.
Hersteller	Zeigt den Herstellernamen an.
Seriennummer	Zeigt die Hersteller-Seriennummer an.
Manufacture Date	Zeigt das Herstellungsdatum an.

30

Anzeigen der Hardware: Prozessordetails für Datacenter oder Cluster

Zeigen Sie die Prozessordetails für Datacenter oder Cluster im Dell Datacenter/Cluster Informationen-Register an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Datacenter oder Cluster" das spezifische Datacenter oder den Cluster aus, für das/den Sie die Prozessordetails anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen" das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister „Hardware: Prozessor" Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer an.
Sockel	Zeigt die Steckplatznummer an.
Geschwindigkeit	Zeigt die aktuelle Geschwindigkeit an.
Marke	Zeigt die Prozessormarke an.
Version	Zeigt die Prozessorversion an.
Kerne	Zeigt die Anzahl der Prozessorkerne an.

31

Anzeigen der Hardware: Netzteil-Details für Datacenter und Cluster

Zeigen Sie die virtuellen Netzteildetails für Datacenter oder Cluster im Register Dell Datacenter-/ Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Hardware: Netzteildetails anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: Netzteil** Folgendes anzeigen:

Host — Zeigt den Namen des Hosts an.

Service Tag — Zeigt die Service-Tag-Nummer an.

Typ — Zeigt den Netzteiltyp an. Die Netzteiltypen beinhalten folgendes:

- UNBEKANNT
- LINEAR
- SCHALTNETZTEIL
- BATTERY
- USV
- UMWANDLER
- REGULATOR
- Wechselstrom (AC)
- Gleichstrom (DC)
- VRM

Standort — Zeigt den Standort des Netzteils an, z.B. Steckplatz 1.

Ausgabe (Watt) — Zeigt die Stromkapazität in Watt an.

Status — Zeigt den Status des Netzteils an. Die Statusoptionen beinhalten folgendes:

- ANDERE
- UNBEKANNT
- OK
- KRITISCH
- NICHT KRITISCH
- WIEDERHERSTELLBAR

- NICHT WIEDERHERSTELLBAR
- HOCH
- NIEDRIG

32

Anzeigen der Hardware: Speicherdetails für Datacenter und Cluster

Zeigen Sie die Speicherdetails für Datacenter oder Cluster im Register Dell Datacenter-/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine CSV-Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Hardware: Speicher-Details anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: Speicher** Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Steckplatz	Zeigt den DIMM-Steckplatz an.
Größe	Zeigt die Speichergröße an.
Typ	Zeigt den Speichertyp an.

33

Anzeigen der Hardware: NICs-Details für Datacenter und Cluster

Zeigen Sie die Details für die Netzwerkschnittstellenkarte (NIC) für Datacenter oder Cluster im Register Dell Datacenter-/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine CSV-Datei exportieren. Diese Seiten bieten Filter- und Suchfunktionen auf dem Datengitter an. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Hardware: NIC-Details anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: NICs** Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Name	Zeigt den NIC-Namen an.
Hersteller	Zeigt nur den Herstellernamen an.
MAC-Adresse	Zeigt die MAC-Adresse der NIC an.

34

Anzeigen der Hardware: PCI-Steckplatzdetails für Datacenter und Cluster

Zeigen Sie die PCI-Steckplatzdetails für Datacenter oder Cluster im Register Dell Datacenter-/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine CSV-Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte" ein spezifisches Datacenter oder einen Cluster aus, für den Sie „Hardware: PCI-Steckplatzdetails" anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen" das Register **Dell Datacenter-/Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: PCI-Steckplätze** Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Steckplatz	Zeigt den Steckplatz an.
Hersteller	Zeigt den Herstellernamen des PCI-Steckplatzes an.
Beschreibung	Zeigt die Beschreibung des PCI-Geräts an.
Typ	Zeigt den Typ des PCI-Steckplatzes an.
Breite	Zeigt die Datenbusbreite an, wenn verfügbar.

35

Hardware-Anzeige: Einzelheiten von Remote-Zugriffskarten

Zeigen Sie die Details der Remote-Zugriffskarte für Datacenter oder Cluster im Register Dell Datacenter-/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte" ein spezifisches Datacenter oder Cluster aus, für das/den Sie die Details der Remote-Zugriffskarten anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen" das Register **Dell Datacenter-/Cluster-Informationen** aus und lassen Sie im Unterregister **Hardware: Remote-Zugriffskarte** Folgendes anzeigen:

Host	Zeigt den Host-Namen an.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer an.
IP-Adresse	Zeigt die IP-Adresse der Remote-Zugriffskarte an.
MAC-Adresse	Zeigt die MAC-Adresse der Remote-Zugriffskarte an.
RAC-Typ	Zeigt den Typ der Remote-Zugriffskarte an.
URL	Zeigt die verfügbare URL für den iDRAC an, der diesem Host zugeordnet wurde.

36

Anzeigen der Hardware: physische Festplatte für Datacenter und Cluster

Zeigen Sie die Details der physischen Festplatte für Datacenter oder Cluster im Register Dell Datacenter-/Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

 **ANMERKUNG:** Hardwareansichten melden die Daten aus OMSA und iDRAC direkt.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte" ein spezifisches Datacenter oder einen Cluster aus, für den Sie „Speicher: Details einer physischen Festplatte" anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen" das Register **Dell Datacenter-/Cluster-Informationen** aus und lassen Sie im Unterregister **Speicher: Physische Festplatte** Folgendes anzeigen:

    **ANMERKUNG:** Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host vom Datengitter aus.

Host	Zeigt den Namen des Hosts an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Kapazität	Zeigt die Kapazität der physischen Festplatte an.
Festplattenstatus	Zeigt den Status der physischen Festplatte an. Die Optionen beinhalten folgendes: • ONLINE • BEREIT • HERABGESETZT • FEHLGESCHLAGEN • OFFLINE • NEUERSTELLUNG • INKOMPATIBEL • ENTFERNT • GELÖSCHT • SMART-WARNUNG FESTGESTELLT • UNBEKANNT • FREMD • NICHT UNTERSTÜTZT

ANMERKUNG: Lesen Sie für weitere Informationen über die Bedeutung dieser Warnungen das *Dell OpenManage™ Server Administrator Storage Management User's Guide* (Dell OpenManage™ Server Administrator Storage Management Benutzerhandbuch), dieses befindet sich auf: http://support.dell.com/support/edocs/software/svradmin/5.1/en/omss_ug/html/adprin.html.

Modellnummer	Zeigt die Modellnummer des physischen Speichergeräts an.
Host	Zeigt den Host-Namen an.
Letzte Bestandsaufnahme	Zeigt den Tag, Monat und die Uhrzeit an, zu der die letzte Bestandsaufnahme ausgeführt wurde.
Status	Zeigt den Host-Status an.
Controller ID	Anzeige der Controller-ID.
Konnektor-ID	Zeigt die Konnektor-ID an.
Gehäuse-ID	Zeigt die Gehäuse-ID an.
Geräte-ID	Anzeige der Geräte-ID.
Busprotokoll	Zeigt das Bus-Protokoll an.
Hotspare-Typ	Zeigt den Hot-Spare-Typ an. Die Optionen beinhalten folgendes: • No Nein bedeutet, dass kein Hot-Spare vorhanden ist. • Global Ein globales Hot-Spare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist. • Dediziert Ein dedizierter Hotspare ist eine nicht verwendete Backup-Festplatte, die einer einzelnen virtuellen Festplatte zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte versagt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen.
Teilenummer	Zeigt die Speicherteilenummer an.
Seriennummer	Zeigt die Speicherseriennummer an.
Herstellername	Zeigt den Speicheranbieternamen an.

37

Speicher anzeigen: Details einer virtuellen Festplatte für Datacenter und Cluster

Zeigen Sie die virtuellen Speicherdetails für ein Datacenter oder einen Cluster auf der Registerkarte „Dell Datacenter/ Cluster“ an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahmen-Job ausführen. Die angezeigten Daten variieren je nach Anzeigeart, mit der Sie auf die Daten zugreifen. Hardware-Ansichten melden die Daten direkt von OMSA und iDRAC. Lesen Sie dazu Sofortige Ausführung eines Bestandsaufnahme-Jobs. Datacenter- und Cluster-Seiten ermöglichen den Export von Informationen in eine CSV-Datei und bieten Filter-/ Suchfunktionen auf dem Datengitter an.

1. Klicken Sie in VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ ein spezifisches Datacenter oder einen Cluster aus, für den Sie „Speicher: Details einer virtuellen Festplatte“ anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter/- Cluster-Informationen** aus und lassen Sie im Unterregister „Speicher: Virtuelle Festplatte“ Folgendes anzeigen:

 **ANMERKUNG:** Um die vollständige Liste von Details anzuzeigen, wählen Sie einen spezifischen Host aus dem Datengitter aus.

Host	Zeigt den Namen des Hosts an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Name	Zeigt den Namen der virtuellen Festplatte an.
Physische Festplatte	Zeigt an, auf welcher physischen Festplatte sich die virtuelle Festplatte befindet.
Kapazität	Zeigt die Kapazität der virtuellen Festplatte an.
Layout	Zeigt den Layout-Typ des virtuellen Speichers an. Damit ist der für diese virtuelle Festplatte konfigurierte RAID-Typ gemeint.
Host	Zeigt den Host-Namen an.
Name	Zeigt den Namen der virtuellen Festplatte an.
Letzte Bestandsaufnahme	Zeigt den Tag, das Datum und die Uhrzeit an, zu dem die Bestandsaufnahme zuletzt durchgeführt wurde.
Controller ID	Anzeige der Controller-ID.
Geräte-ID	Anzeige der Geräte-ID.
Datenträgertyp	Zeigt entweder SSD oder HDD an.
Busprotokoll	Dies zeigt die von den in der virtuellen Festplatte enthaltenen physischen Festplatten verwendete Technologie an. Mögliche Werte sind: • SCSI • SAS

- SATA

Stripe-Größe Die Stripe-Größe bezieht sich auf die Menge an Speicherplatz, die jeder Stripe auf einer einzelnen Festplatte belegt.

Standard-Leserichtlinie Die durch den Controller standardmäßig unterstützte Leserichtlinie. Die Optionen beinhalten:

- Vorauslesen
- Kein Vorauslesen
- Adaptives Vorauslesen
- Lese-Cache aktiviert
- Lese-Cache deaktiviert

Standard-Schreibrichtlinie Die durch den Controller standardmäßig unterstützte Schreibrichtlinie. Die Optionen beinhalten:

- Rückschreiben
- Rückschreiben erzwingen
- Rückschreiben aktiviert
- Durchschreiben
- Schreib-Cache aktiviert und geschützt.
- Schreib-Cache deaktiviert

Festplatten-Cache-Regel Die durch den Controller standardmäßig unterstützte Cacherichtlinie. Die Optionen enthalten:

- Aktiviert
  Damit ist die Cache-E/A gemeint.
- Deaktiviert
  Damit ist die direkte E/A gemeint.

38

Anzeigen von Firmwaredetails für Datacenter und Cluster

Zeigen Sie die Firmwaredetails für Datacenter oder Cluster im Dell-Host-Register an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ einen spezifischen Host, ein Datacenter oder einen Cluster aus, für den Sie die Firmware-Details anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister „Firmware“ Folgendes anzeigen:

Host	Zeigt den Namen des Hosts an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Name	Zeigt den Namen von sämtlicher Firmware auf diesem Host an.
Version	Zeigt die Version von sämtlicher Firmware auf diesem Host an.

39

Anzeigen von Garantiezusammenfassung für Datacenter und Cluster

Sie müssen einen Garantie-Job ausgeführt haben, um eine Garantiezusammenfassung anzuzeigen. Siehe Sofortiges Ausführen eines Garantie-Jobs.
Zeigen Sie die Garantiezusammenfassungsdetails für Datacenter oder Cluster auf dem Register Dell Datacenter-/Cluster Informationen an. Mit Datacenter- und Clusterseiten können Sie Informationen in eine CSV-Datei exportieren und Filter- und Suchfunktionen auf dem Datengitter anbieten. Die Seite Garantiezusammenfassung ermöglicht es Ihnen, durch das Aktivieren oder Deaktivieren des Garantiezeitplans und das Einstellen der Mindesttageschwellenwertwarnung das Garantie-Verfallsdatum zu überwachen und Garantieeinstellungen zu kontrollieren, wenn Servergarantieinformationen von Dell-Online abgerufen werden. Siehe Garantieverlauf.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenter** oder **Cluster**.
3. Wählen Sie im Register „Objekte“ ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Einzelheiten der Garantiezusammenfassung anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen“ das Register **Dell Datacenter-/ Cluster-Informationen** aus und lassen Sie im Unterregister „Garantiezusammenfassung“ Folgendes anzeigen:

Garantiezusammenfassung	Der Host-Garantiezusammenfassung wird mithilfe von Symbolen angezeigt, um die Anzahl der Hosts in jeder Statuskategorie visuell anzuzeigen.
Host	Zeigt den Namen des Hosts an.
Service Tag	Zeigt die Service-Tag-Nummer des Hosts an.
Beschreibung	Zeigt eine Beschreibung an.
Garantiestatus	Zeigt den Garantiestatus des Hosts an. Die Statusoptionen beinhalten: • Aktiv Der Host ist unter Garantie und hat keinen Schwellenwert überschritten. • Warnung Der Host ist aktiv, hat jedoch den Warnungsschwellenwert überschritten. • Kritisch Entspricht einer Warnung, jedoch für einen kritischen Schwellenwert. • Abgelaufen Die Garantie für diesen Host ist abgelaufen. • Unbekannt OpenManage Integration for VMware vCenter kann den Garantiestatus nicht abrufen, weil der Garantieauftrag nicht ausgeführt wurde, ein Fehler beim Abrufen der Daten aufgetreten ist, oder weil das System keine Garantie hat.
Verbleibende Tage	Zeigt die verbleibende Garantiezeit in Tagen an.

40 Anzeigen von Stromüberwachung für Datacenter und Cluster

Zeigen Sie die Stromüberwachungdetails für Datacenter oder Cluster im Register Dell Datacenter-/ Cluster-Informationen an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Mit Datacenter- und Clusterseiten können Sie Informationen in eine Datei exportieren, und Filter- und Suchfunktionen auf dem Datengitter anbieten. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie im VMware vCenter im Navigator auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register „Objekte" ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Details der Stromüberwachung anzeigen lassen wollen.
4. Wählen Sie im Register „Überwachen" das Register **Dell Datacenter-/ Cluster-Informationen-Host** aus und lassen Sie auf dem Unterregister „Stromüberwachung" Folgendes anzeigen:

   ANMERKUNG: Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host vom Datengitter aus.

Host	Zeigt den Namen des Hosts an.
Service Tag	Zeigt die Service-Tag-Nummer an.
Aktuelles Profil	Zeigt das Stromprofil zur Maximierung der Systemleistung und zum Stromsparen an.
Energieverbrauch	Zeigt den Energieverbrauch des Hosts an.
Spitzenreservekapazität	Zeigt die Spitzenstromreservekapazität an.
Power Budget	Zeigt die Stromobergrenze dieses Hosts an.
Warnungsschwelle	Zeigt den konfigurierten Maximalwert für den Warnungsschwellenwert der Temperatursonden des Systems an.
Fehlerschwelle	Zeigt den konfigurierten Maximalwert für den Fehlerschwellenwert der Temperatursonden des Systems an.
Sofortige Reservekapazität	Zeigt die Kapazität des sofortigen Toleranzbereichs des Hosts an.
Startdatum des Energieverbrauchs	Zeigt das Datum und die Uhrzeit an, zu der der Host mit dem Energieverbrauch begonnen hat.
Enddatum des Energieverbrauchs	Zeigt das Datum und die Uhrzeit an, zu der der Energieverbrauch des Hosts gestoppt wurde.
Spitzenleistung des Systems	Zeigt die Spitzenleistung des Hosts an.

Startdatum der Spitzenleistung des Systems	Zeigt das Datum und die Uhrzeit an, zu der die Spitzenleistung des Hosts begonnen hat.
Enddatum der Spitzenleistung des Systems	Zeigt das Datum und die Uhrzeit an, zu der die Spitzenleistung des Hosts beendet wurde.
Spitzen-Ampere des Systems	Zeigt die Spitzen-Ampere des Hosts an.
Startdatum der Spitzen-Ampere des Systems	Zeigt das Datum und die Uhrzeit des Beginns der Host-Spitzen-Ampere an.
Enddatum der Spitzen-Ampere des Systems	Zeigt das Datum und die Uhrzeit an, zu der die Spitzen-Ampere des Hosts beendet wurden.

41

Konsolenverwaltung

Es gibt zwei Konsolen, die Sie mit OpenManage Integration for VMware vCenter für administrative Tasks des Geräts verwenden, die VMware vCenter-Konsole und die Administration Console. Die VMware vCenter-Konsole wird zuerst während des Setup und der Registrierung von OpenManage Integration for VMware vCenter verwendet. Später können Sie sie zur Konfiguration von Netzwerkeinstellungen und einer Liste weiterer Funktionen verwenden. Einige der Tasks, die Sie auf der VMware vCenter-Konsole ausführen können, können Sie auch in der Administration Console ausführen. Siehe Verstehen der vCenter-Konsole. Nach dem Setup und der Registrierung verwalten Sie das virtuelle Gerät für die meisten Verwaltungs-Tasks mit der Administration Console. Mit der Administration Console können Sie Folgendes ausführen:

- Registrieren eines vCenter-Servers
- Modifizieren der vCenter Administrator-Anmeldung
- Aktualisieren der SSL-Zertifikate für registrierte vCenter
- Deinstallieren von OpenManage Integration for VMware vCenter von vCenter
- Hochladen der OpenManage Integration for VMware vCenter zum administrativen Portal
- Neustarten des virtuellen Geräts
- Aktualisieren eines Repository-Speicherorts und eines Geräts
- Aktualisieren der Softwareversion des virtuellen Geräts
- Herunterladen eines Fehlerbehebungsbündels
- Einrichten des HTTP-Proxys mithilfe der Administrator-Konsole
- Einrichten der NTP-Server
- Erzeugen einer Zertifikatsignierungsanforderung
- Wiederherstellen des standardmäßigen HTTPS-Zertifikats
- Einrichten globaler Alarme
- Verwalten von Backups und Wiederherstellungen

Registrieren eines vCenter-Servers

Sie können OpenManage Integration für VMware vCenter nach der Installation von OpenManage Integration for VMware vCenter registrieren. OpenManage Integration for VMware vCenter verwendet das Admin-Benutzerkonto für vCenter-Vorgänge. OpenManage Integration for VMware vCenter unterstützt 10 vCenters pro Gerät.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie zum Registrieren eines neuen Servers im linken Fensterbereich auf **VCENTER REGISTRIERUNG** und dann auf **Neuen vCenter-Server registrieren**.

4. Führen Sie im Dialogfeld **Neues vCenter registrieren** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder ein FQDN des Hosts in das Textfeld **vCenter-Server-IP-Adresse oder Hostname** ein.
   b. Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
5. Unter **Admin-Benutzerkonto** führen Sie die folgenden Schritte aus:
   a. Geben Sie den Benutzernamen des Administrators in das Textfeld **Admin-Benutzername** ein.
   b. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   c. Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
6. Klicken Sie auf **Registrieren**.

Anforderungen für OpenManage Integration for VMware vCenter

Die OpenManage Integration for VMware vCenter (OMIVV) erfordert Informationen von OpenManage auf Servern einer älteren Generation und neuere Plattformen sind darauf beschränkt, mit der Version von vSphere zu starten, die den neueren Chipsatz versteht. Daher gibt es Beschränkungen in Bezug auf die Version von vSphere, mit der eine bestimmte Version von OMIVV arbeitet.

ESXi-Versionen, die auf verwalteten Hosts unterstützt werden sollten:

ESX/ESXi-Version-Unterstützung	Plattform-Generation-Support				
	9G	10G	11G	12G	13G
v4.1 (ESX/ESXi)	J	J	J	N	N
v4.1 U1 (ESX/ESXi)	J	J	J	N	N
v4.1 U2 (ESX/ESXi)	J	J	J	J	N
v4.1 U3 (ESX/ESXi)	J	J	J	J	N
v5.0	J	J	J	J	N
v5.0 U1	J	J	J	J	N
v5.0 U2	J	J	J	J	N
v5.0 U3	J	J	J	J	N
v5.1	J	J	J	J	N
v5.1 U1	J	J	J	J	N
v5.1 U2	J	J	J	J	N
v5.5	N	j	J	J	N
v5.5 U1	N	N	N	N	J
v5.5 U2	N	N	N	J	J

vCenter sSupport

Derzeit ist die Unterstützung für v5.5 U1 nur mit Servern der 12. Generation über iDRAC mit Lifecycle Controller-Unterstützung verfügbar. OpenManage-Support für 5.5 U1 mit Servern der älteren Generation ist in Kürze zu erwarten. vSphere v5.5 U1 wird mit dem aktuellen Chipsatz nicht unterstützt, so wird es auf den Plattformen der 13. Generation auch nicht unterstützt.

Unterstützung für vSphere v5.5 U2

Mit der Unterstützung von iDRAC mit Lifecycle Controller 5.5 U2 wird vSphere für Plattformen der 12. und 13. Generation unterstützt.

Unterstützte vCenter Server-Versionen für Version 2.3

Die OpenManage Integration for VMware vCenter arbeitet mit jeder dieser vCenter Server-Versionen:

vCenter-Version	Desktop-Client-Support	Web-Client-Support
v5.0 U3	J	N
5.1 U2	J	N
v5.5	J	J
v5.5 U1	J	J
v5.5 U2	J	J

Mit jeder gegebenen vCenter-Version müssen die ESX / ESXi-Hosts, die es verwaltet, über eine gleiche oder niedrigere Version verfügen. Um eine vSphere v4.1- oder v5.0-Umgebung mit OMIVV zu verwalten, müssen Sie über eine vCenter-Mindestversion v5.0 U3 verfügen.

Modifizieren der vCenter Administrator-Anmeldung

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden im rechten Fensterbereich angezeigt. Klicken Sie zum Öffnen des Fensters **Admin-Konto modifizieren** unter **Anmeldeinformationen** auf **Modifizieren**.
4. Geben Sie den **Benutzername** und das **Kennwort** für den vCenter Administrator ein, und bestätigen Sie das Kennwort unter **Kennwort bestätigen**.
5. Klicken Sie auf **Anwenden**, um das Kennwort zu ändern, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren der SSL-Zertifikate für registrierte vCenter-Server

Wenn das SSL-Zertifikat auf einem vCenter-Server geändert wird, führen Sie die folgenden Schritte aus, um das neue Zertifikat für das OpenManage Integration for VMware vCenter zu importieren. DasOpenManage Integration for VMware vCenterr verwendet dieses Zertifikat, um sicherzustellen, dass der vCenter-Server mit dem richtigen vCenter-Server und nicht mit einem Nachahmer kommuniziert.

OpenManage Integration for VMware vCenter verwendet das openssl API zum Erstellen des Certificate Signing Request (CSR) unter Verwendung des RSA-Verschlüsselungsstandards mit einer 2048 Bitschlüssellänge. Das durch OpenManage Integration for VMware vCenter erstellte CRS erhält ein digital signiertes Zertifikat einer vertrauenswürdigen Zertifizierungsstelle. Das OpenManage Integration for VMware vCenter verwendet das digitale Zertifikat zum Aktivieren von SSL auf dem Webserver für eine sichere Kommunikation.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAdrdress> ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenters werden im rechten Fensterbereich angezeigt. Zur Aktualisierung der Zertifikate klicken Sie auf **Aktualisieren**.

Deinstallieren des OpenManage Integration for VMware vCenter von VMware vCenter

Um das OpenManage Integration for VMware vCenter zu entfernen, müssen Sie die Registrierung des vCenter-Servers unter Verwendung der Administrationskonsole aufheben.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Heben Sie auf der Seite **vCenter Registrierung** unter der vCenter-Server-Tabelle die Registrierung der OpenManage Integration for VMware vCenter durch das Klicken auf **Registrierung aufheben** auf.

   Wenn Sie mit mehreren vCentern arbeiten, achten Sie darauf, das richtige auszuwählen.
4. Wenn Sie im Dialogfeld **vCenter-Registrierung aufheben** gefragt werden, ob Sie die Registrierung dieses Servers aufheben möchten, klicken Sie auf **Registrierung aufheben**.

Hochladen einer OpenManage Integration for VMware vCenter-Lizenz auf die Administrationskonsole

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden in einer Tabelle angezeigt. Klicken Sie zum Anzeigen des Dialogfelds „Lizenz hochladen" auf **Lizenz hochladen**.
4. Um zur Lizenzdatei zu navigieren, klicken Sie auf die Schaltfläche **Durchsuchen** und dann auf **Hochladen**.

   ANMERKUNG: Falls die Lizenzdatei irgendwie geändert oder bearbeitet wurde, sieht das Gerät sie als korrupt an, und die Datei funktioniert nicht. Sie können Lizenzen hinzufügen, wenn Sie mehr Hosts hinzufügen müssen. Befolgen Sie den obigen Vorgang, um weitere Lizenzen hinzuzufügen.

   ANMERKUNG: Wenn die Anzahl der erfolgreich inventarisierten Server der 11., 12. und 13. Generation der Anzahl der erworbenen Lizenzen entspricht, wird das Hinzufügen von Servern der 9. und 10. Generation zu neuen oder vorhandenen Verbindungsprofilen blockiert. Bearbeiten Sie vorhandene Verbindungsprofile, indem Sie einige Server der 11., 12., 13. Generation entfernen und stattdessen Server der 9. oder 10. Generation hinzufügen. Erstellen Sie ein neues Verbindungsprofil für die entfernten Server der 11., 12. oder 13. Generation.

Neustarten des virtuellen Geräts

Das Neustarten des virtuellen Gerät meldet Sie von der Administration Console ab und das OpenManage Integration for VMware vCenter ist nicht mehr verfügbar, bis das virtuelle Gerät und seine Dienste aktiv sind.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Zu Neustart des OpenManage Integration for VMware vCenter klicken Sie auf **Neustarten des virtuellen Geräts**.
5. Klicken Sie im Dialogfeld **Virtuelles Gerät neustarten** auf **Anwenden**, um das virtuelle Gerät neu zu starten, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren eines Repository-Speicherorts und virtuellen Geräts

Führen Sie vor dem Aktualisieren des virtuelle Geräts ein Backup aus, um sicherzustellen, dass alle Daten geschützt sind. Siehe Verwalten von Backups und Wiederherstellungen.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie neben „Geräteaktualisierung“ auf **Bearbeiten**.
5. Im Fenster **Geräteaktualisierung** geben Sie die **Repository-Standort URL** ein und klicken Sie auf **Anwenden**.



ANMERKUNG: Wenn sicher der Aktualisierungsspeicherort in einem externen Netzwerk befindet (z. B. der Dell FTP-Site), muss ein Proxyserver im Bereich „HTTP Proxy“ angegeben werden.

Aktualisieren der Softwareversion des virtuellen Geräts

Erstellen Sie vor der Softwareaktualisierung ein Backup der Daten auf dem virtuellen Gerät, um einen möglichen Datenverlust vermeiden.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEWARTUNG**.
3. Klicken Sie zum Aktualisieren der Softwareversion des virtuellen Geräts unter **Geräteaktualisierung** auf **Virtuelles Gerät aktualisieren**.
4. Im Dialogfeld **Gerät aktualisieren** werden die aktuelle und die verfügbare Versionen aufgeführt. Klicken Sie auf **Aktualisieren**, um die Aktualisierung zu beginnen.
5. Das System wird gesperrt und in den Wartungsmodus versetzt. Nachdem die Aktualisierung abgeschlossen ist, zeigt die Seite „Gerät“ die neu installierte Version an.

Einrichten des HTTP-Proxy

Sie können die HTTP-Proxy-Einstellungen entweder in der Administrator Console oder in der Dell Management Console einrichten.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Scrollen Sie auf der Seite **Geräteverwaltung** bis zu **HTTP-Proxy-Einstellungen** und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie auf der Seite **Bearbeiten** die folgenden Schritte aus:
   a. Wählen Sie neben **HTTP-Proxy-Einstellungen verwenden** die Option **Aktivieren**.
   b. Geben Sie die Proxyserver-Adresse in das Textfeld **Proxyserver-Adresse** ein.
   c. Geben Sie den Proxyserver-Port in das Textfeld **Proxyserver-Schnittstelle** ein.
   d. Wählen Sie neben **Proxy-Anmeldeinformationsnachweis verwenden** die Option **Ja**, um die Proxy-Anmeldeinformationen zu verwenden.
   e. Wenn Sie ie Anmeldeinformationen verwenden, geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   f. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
6. Klicken Sie auf **Anwenden**.

Einrichten der NTP-Server

Verwenden Sie das Network Time Protocol (NTP) zum Synchronisieren der Uhren der virtuellen Geräte mit der Uhr eines NTP-Servers.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung“ in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Für NTP bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen **Aktiviert**. Geben Sie den **Hostnamen** oder die **IP-Adresse** für einen **bevorzugten** und einen **sekundären NTP-Server** ein und klicken Sie auf **Anwenden**.
6. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Erzeugen einer Zertifikatsignierungsanforderung



ANMERKUNG: Sie müssen das Zertifikat vor der Registrierung des OpenManage Integration for VMware vCenter mit vCenter hochladen.

Das Erzeugen einer Zertifikatsignierungsanforderung verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikatsignierungsanforderung für HTTPS-Zertifikate erzeugen**. Eine Meldung zeigt an, dass wenn eine neue Anforderung erzeugt wird, mit dem vorherigen CSR erzeugte Zertifikate nicht mehr auf das Gerät hochgeladen werden. Klicken Sie zum Fortsetzen der Anforderung auf **Weiter**, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.
5. Geben Sie den **Allgemeinen Namen,Name der Organisation**, **Organisationseinheit**, **Standort**, **Name des Bundeslands/der Provinz**, **Land** und **E-Mail-Adresse** für die Anforderung ein. Klicken Sie dann auf **Fortsetzen**.
6. Klicken Sie auf **Herunterladen**, dann speichern Sie das resultierende HTTPS-Zertifikat an einem zugänglichen Speicherort.

Hochladen eines HTTPS-Zertifikats

HTTPS-Zertifikate werden für die sichere Kommunikation zwischen dem virtuellen Gerät und Hostsystemen verwendet. Um diese sichere Kommunikation einzurichten, muss eine Zertifikatssignierungsanfrage an eine Zertifizierungsstelle gesendet werden, dann wird das resultierende Zertifikat mithilfe der Administration Console hochgeladen. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.



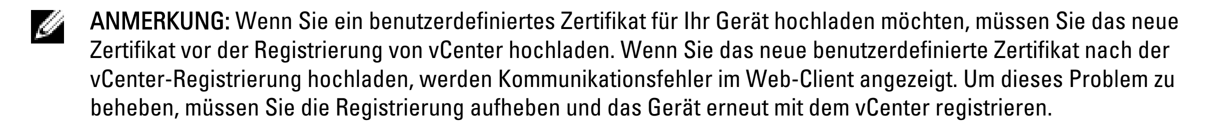
ANMERKUNG: Sie können entweder Microsoft Internet Explorer, Firefox oder Chrome verwenden, um Zertifikate hochzuladen.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikat für HTTPS-Zertifikate hochladen**.

5. Klicken Sie im Dialogfeld **Zertifikate hochladen** auf **OK**.
6. Klicken Sie zum Auswählen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
7. Klicken Sie auf **Abbrechen**, wenn Sie das Hochladen abbrechen müssen.

   ANMERKUNG: Das Zertifikat muss im PEM-Format vorliegen.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats



ANMERKUNG: Wenn Sie ein benutzerdefiniertes Zertifikat für Ihr Gerät hochladen möchten, müssen Sie das neue Zertifikat vor der Registrierung von vCenter hochladen. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden Kommunikationsfehler im Web-Client angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung aufheben und das Gerät erneut mit dem vCenter registrieren.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Standardmäßiges Zertifikat für HTTPS-Zertifikate wiederherstellen**.
5. Klicken Sie im Dialogfeld „Standardmäßiges Zertifikat wiederherstellen“ auf **Anwenden**.

Einrichten globaler Alarme

Mit der Alarmverwaltung können Sie globale Einstellungen, wie Alarme für alle vCenter-Instanzen gespeichert werden, festlegen.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung“ in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **ALARMVERWALTUNG**. Klicken Sie auf **Bearbeiten**, um neue vCenter-Alarmeinstellungen festzulegen.
4. Geben Sie numerische Werte für die folgenden Elemente ein:
   - Maximale Anzahl an Alarmen
   - Anzahl an Tagen, über die Alarme beibehalten werden sollen
   - Timeout für duplizierte Alarme (Sekunden)
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Verwalten von Backups und Wiederherstellungen

Die Verwaltung von Backups und Wiederherstellungen erfolgt über die Administrator Console. Die Tasks auf dieser Seite umfassen:

- Konfigurieren von Backup und Wiederherstellung
- Planen von automatischen Backups
- Durchführen eines sofortigen Backups
- Wiederherstellen der Datenbank aus einem Backup

Konfigurieren von Backup und Wiederherstellung

Die Funktionen für das Backup und die Wiederherstellung sichern die Datenbank des OpenManage Integration for VMware vCenter an einem remoten Speicherort, von dem aus sie zu einem späteren Zeitpunkt wieder hergestellt

werden kann. Profile, Vorlagen und Host-Informationen sind im Backup eingeschlossen. Wir empfehlen, dass Sie zum Schutz gegen Datenverlust automatische Backups planen. Nach diesem Verfahren müssen Sie einen Backup-Zeitplan konfigurieren.

ANMERKUNG: NTP-Einstellungen werden nicht gesichert.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Bearbeiten**, um die aktuellen Einstellungen für Backup und Wiederherstellung zu bearbeiten.
5. Führen Sie auf der Seite **Einstellungen und Details** die folgenden Schritte aus:
   a. Geben Sie den Pfad zu den gesicherten Dateien in das Textfeld **Speicherort des Backups** ein.
   b. Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   d. Geben Sie das Verschlüsselungskennwort in das Textfeld **Kennwort für die Verschlüsselung von Backups** ein.

      Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
   e. Geben Sie das Verschlüsselungskennwort erneut in das Textfeld **Kennwort bestätigen** ein.
6. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.
7. Konfigurieren Sie den Backup-Zeitplan. Weitere Informationen finden Sie unter Planen von automatischen Backups.

Planen von automatischen Backups

Dies ist der zweite Teil der Konfiguration von Backup und Wiederherstellung. Ausführliche Informationen zum Konfigurieren des Backup-Speicherorts und des Berechtigungsnachweises finden Sie unter Konfigurieren von Backup und Wiederherstellung.
So konfigurieren Sie ein automatisches Backup:

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Bearbeiten Automatisch geplanter Backup**, um die Einstellungen für Backup und Wiederherstellung zu ändern. Das Feld wird aktiviert.
5. Klicken Sie auf **Aktiviert**, um Backups zu aktivieren.
6. Aktivieren Sie die Kontrollkästchen der Tage, an denen ein Backup durchgeführt werden soll .
7. Geben Sie die Zeit in dem Format HH:MM in das Textfeld **Uhrzeit für Backup (24 Stunden Uhrzeitformat, HH:mm)** ein.

   Das Feld **Nächster Backup** wird mit dem Datum und der Uhrzeit für den nächsten geplanten Backup ausgefüllt.
8. Klicken Sie auf **Anwenden**.

Durchführen eines sofortigen Backups

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
4. Klicken Sie auf **Jetzt sichern**.

5. Aktivieren Sie im Dialogfeld **Jetzt sichern** das entsprechende Kontrollkästchen, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
6. Geben Sie einen **Speicherort für das Backup**, einen **Benutzernamen**, ein **Kennwort** und das **Verschlüsselungskennwort** ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
7. Klicken Sie auf **Sichern**.

Wiederherstellen der Datenbank aus einem Backup

ANMERKUNG: Bei einer Wiederherstellung wird das virtuelle Geräte nach Abschluss der Wiederherstellung neu gestartet wird.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administration Console.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**. Die aktuellen Einstellungen für das Backup und die Wiederherstellung werden angezeigt.
4. Klicken Sie auf **Jetzt wiederherstellen**.
5. Geben Sie einen **Dateispeicherort (CIFS/NFS-Format)** in das Dialogfeld „Jetzt wiederherstellen" ein.
6. Geben Sie den **Benutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
7. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

   Das Gerät wird neu gebootet oder startet neu, nachdem Sie auf „Anwenden" geklickt haben.

Grundlegendes zur vSphere Client-Konsole

Die **Konsole** befindet sich innerhalb des vSphere-Clients auf einer virtuellen Maschine. Die **Konsole** arbeitet Hand in Hand mit der Administrationskonsole. Die Konsole ermöglicht die Ausführung folgender Aufgaben:

- Konfiguration von Netzwerkeinstellungen
- Ändern des Kennworts des virtuellen Geräts
- Einstellen der lokalen Uhrzeit
- Neustart des virtuellen Geräts
- Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen
- Aktualisieren der Konsole
- Option Abmelden

Verwenden Sie die Pfeiltasten, um nach oben oder unten zu navigieren. Wenn Sie die gewünschte Option einmal ausgewählt haben, drücken Sie die <EINGABETASTE>. Wenn Sie auf den **Konsole**nbildschirm zugreifen, übernimmt der VMware vSphere-Client die Kontrolle Ihres Cursors. Um dieser Kontrolle zu entgehen, drücken Sie **<STRG> + <ALT>**.

Konfigurieren der Netzwerkeinstellungen

Die Netzwerkeinstellungen werden im vSphere-Client auf der Konsole eingerichtet.

1. Wählen Sie im vSphere-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
    - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Wählen Sie im Fenster **Konsole** die Option **Netzwerk konfigurieren** und drücken Sie die **<EINGABETASTE>**.
5. Geben Sie die gewünschten Netzwerkeinstellungen unter **Geräte bearbeiten** oder unter **DNS bearbeiten** ein und klicken Sie auf **Speichern und Beenden**. Klicken Sie auf **Beenden**, um die Änderungen zu verwerfen.

Ändern des Kennworts des virtuellen Geräts

Das Kennwort des virtuellen Geräts wird im vSphere Web-Client auf der Registerkarte „Konsole“ geändert.

1. Wählen Sie im vSphere Web-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
    - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Wählen Sie in der Konsole mit den Pfeiltasten die Option **Admin-Kennwort ändern** aus und drücken Sie die **<EINGABETASTE>**.
5. Geben Sie das **Aktuelle Admin-Kennwort** ein und drücken Sie die **<EINGABETASTE>**.

   Admin-Kennwörter müssen ein Sonderzeichen, eine Zahl, einen Großbuchstaben, einen Kleinbuchstaben und mindestens acht Buchstaben umfassen.
6. Geben Sie ein neues Kennwort unter **Neues Admin-Kennwort eingeben** ein und drücken Sie die **<EINGABETASTE>**.
7. Geben Sie das neue Kennwort erneut in das Textfeld **Admin-Kennwort bestätigen** ein und drücken Sie die **<EINGABETASTE>**.

Einstellen der lokalen Uhrzeit

So stellen Sie die lokale Uhrzeit ein:

1. Führen Sie einen der folgenden Vorgänge aus:
    - Wählen Sie im **vSphere-Client** die virtuelle OpenManage Integration for VMware vCenter-Maschine aus, und klicken Sie dann auf die Registerkarte **Konsole**
    - Wählen Sie **Zeitzone einstellen** und drücken Sie die **<EINGABETASTE>**.
2. Wählen Sie im Fenster **Zeitzonenauswahl** die gewünschte Zeitzone aus und klicken Sie auf **OK**. Um Änderungen zu verwerfen, klicken Sie auf **Abbrechen**. Die Zeitzone wird aktualisiert. Sie können nur die Zeitzone bearbeiten, aber nicht die aktuelle Uhrzeit oder das Datum

Neustarten des virtuellen Geräts

So starten Sie das virtuelle Gerät neu:

1. Wählen Sie im vSphere Web-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Verwenden Sie die Pfeiltasten zur Auswahl von **Dieses virtuelle Gerät neu starten** und drücken Sie die **<EINGABETASTE>**.
5. Die folgende Meldung wird angezeigt:
   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
6. Drücken Sie **j**, um den Neustart fortzusetzen, oder drücken Sie **n**, um den Vorgang abzubrechen. Das Gerät wird neu gestartet.

Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen

So setzen Sie das virtuelle Gerät auf die werkseitigen Einstellungen zurück:

1. Wählen Sie im vSphere-Client im Navigator **vCenter**.
2. Wählen Sie im Navigator die virtuelle Maschine, die Sie verwalten möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Wählen Sie auf dem Objektregister **Maßnahme** → **Konsole öffnen**.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.
4. Verwenden Sie die Pfeiltasten, um **Dieses virtuelle Gerät auf werkseitige Einstellungen zurücksetzen** auszuwählen, und drücken Sie auf die **<EINGABETASTE>**.
5. Die folgende Meldung wird angezeigt:
   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```
6. Geben Sie **y** zum Zurücksetzen oder **n** zum Abbrechen ein. Das Gerät wird auf die ursprünglichen werksseitigen Standardeinstellungen zurückgesetzt und alle anderen Einstellungen und gespeicherten Daten gehen dabei verloren.

    **ANMERKUNG:** Wenn das virtuelle Gerät auf die werkseitigen Einstellungen zurückgesetzt wird, werden alle Aktualisierungen an der Netzwerkkonfiguration beibehalten; diese Einstellungen werden nicht zurückgesetzt.

Aktualisieren der Konsolenansicht

Wählen Sie **Aktualisieren**, um die Konsolenansicht zu aktualisieren, und drücken Sie die **<EINGABETASTE>**.

Schreibgeschützte Benutzerrolle

Es gibt eine Benutzerrolle ohne Rechte mit der Bezeichnung „Nur-Lesen“ mit Shell-Zugriff für Diagnosezwecke. Der Nur-Lesen-Benutzer verfügt über eingeschränkte Rechte zum Ausführen der eingehängten Geräte. Das Kennwort des Nur-Lesen-Benutzers entspricht dem des Administrators.

42

Troubleshooting

Verwenden Sie diesen Abschnitt, um Antworten auf Fragen zur Fehlerbeseitigung zu finden. Dieser Abschnitt umfasst:

- Häufig gestellte Fragen (FAQs)
- Probleme bei der Bare-Metal-Bereitstellung
- Kontaktaufnahme mit Dell
- Zugehörige Produktinformationen

Häufig gestellte Fragen (FAQs)

In diesem Abschnitt werden einige allgemeine Fragen und Lösungen beschrieben.

Das Laden der Seite „Einstellungen“ schlägt nach dem Wechseln der Seite und dem Navigieren zurück zur Seite „Einstellungen“ fehl.

Wenn Sie vom Web Client auf eine andere Seite navigieren und danach zurück zur Seite „Einstellung“ gehen, schlägt das Laden der Seite manchmal fehl. Dies ist ein Aktualisierungsfehler und die Seite wird nicht korrekt aktualisiert.

Lösung: Klicken Sie auf die globale Aktualisierung und der Bildschirm wird korrekt aktualisiert.

Betroffene Versionen: 2.2 und 2.3

Warum werden die DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn für die Geräte-IP DHCP verwendet und die DNS-Einstellungen überschrieben werden?

Es ist ein bekannter Fehler, dass statisch zugewiesene DNS-Einstellungen durch die Werte aus dem DHCP ersetzt werden. Das kann vorkommen, wenn DHCP zum Bezug der IP-Einstellungen verwendet wird und DNS-Werte statisch zugewiesen werden. Wenn der DHCP-Lease verlängert oder das System neu gestartet wird, werden die zugewiesenen DNS-Einstellungen entfernt. Lösung: IP-Einstellungen statisch zuweisen, wenn sich die DNS-Servereinstellungen von DHCP unterscheiden.

Betroffene Version: Alle

Die Verwendung von OpenManage Integration for VMware vCenter zum Aktualisieren einer Intel-Netzwerkkarte mit der Firmwareversion 13.5.2 wird nicht unterstützt.

Es gibt ein bekanntes Problem mit der 12. Generation der Dell PowerEdge-Server und einigen Intel-Netzwerkkarten mit der Firmwareversion 13.5.2. Das Aktualisieren einiger Intel-Netzwerkkartenmodelle mit dieser Firmwareversion schlägt fehl, wenn die Firmware-Aktualisierung mithilfe von Lifecycle Controller durchgeführt wird. Kunden, die diese Firmwareversion verwenden, müssen die Netzwerktreibersoftware mithilfe eines Betriebssystems aktualisieren. Wenn die Firmwareversion der Intel-Netzwerkkarte eine andere ist als 13.5.2, können Sie die Aktualisierung mithilfe von OpenManage Integration for VMware vCenter durchführen. Weitere Informationen finden Sie unter http://

en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx.



ANMERKUNG: Hinweis: Wählen Sie bei der Anwendung einer Firmware-Aktualisierung vom Typ 1:n keine Intel-Netzwerkadapter der Version 13.5.2 aus. Anderenfalls schlägt die Aktualisierung fehl und die Aktualisierungsaufgabe für die verbleibenden Server wird gestoppt.

Beim Versuch einer Firmware-Aktualisierung mit einer ungültigen DUP fällt der Hardware-Job-Status auf der vCenter-Konsole stundenlang weder aus noch weist er eine Zeitüberschreitung auf. Der Job-Status in LC zeigt aber dennoch „FEHLGESCHLAGEN" an. Warum ist das so?

Wenn die ungültige DUP für die Firmware-Aktualisierung abgerufen wird, bleibt der Status der Aufgabe im vCenter-Konsolen-Fenster auf „In Progress" (In Bearbeitung), die Meldung wird jedoch auf die Ursache des Fehlers geändert. Dies ist ein bekannter Fehler von VMWare und wird in zukünftigen Versionen von VMware vCenter behoben.

Lösung: Die Aufgabe muss manuell abgebrochen werden.

Betroffene Version: Alle

Administration-Portal zeigt immer noch den nicht erreichbaren Aktualisierungs-Repository-Speicherort an.

Wenn der vom Benutzer bereitgestellte Aktualisierungs-Repository-Pfad nicht erreichbar ist, wird die Fehlermeldung „Failed: Fehler beim Herstellen einer Verbindung mit der URL..." oben in der System-Aktualisierungsansicht angezeigt, jedoch wird der Aktualisierungs-Repository-Pfad nicht auf den Wert vor der Aktualisierung zurückgesetzt.

Lösung: Gehen Sie von dieser Seite auf eine andere Seite und stellen Sie sicher, dass die Seite aktualisiert wird.

Betroffene Version: Alle

Warum wird der Fehler „Task kann nicht in der Vergangenheit geplant werden" auf der Bestandsaufnahme-Zeitplan/Garantie-Zeitplan-Seite beim Assistenten zur Erstkonfiguration angezeigt?

Wenn der Benutzer im Web-Client „Alle registrierten vCenter" im erstmaligen Konfigurationsassistenten auswählt und sollten einige vCenter ohne Hosts sein oder haben vCenter bereits Bestandsaufnahme- oder Garantie-Tasks geplant und einige vCenter haben noch nichts geplant, wird dem Benutzer manchmal der Fehler „Task kann nicht in der Vergangenheit geplant werden" angezeigt.

Lösung: Sollten einige vCenter über keinen Host verfügen oder sollten Sie vCenter mit bereits geplanten Bestandsaufnahme- oder Garantie-Tasks haben und einige vCenter haben noch nichts geplant, führen Sie die Einstellungen zu dem Bestandsaufnahme- und Garantiezeitplan separat von der Einstellungsseite für diese vCenter aus.

Betroffene Versionen: 2.2 und 2.3

Warum ist mein System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Wartungsmodus gewechselt?

Bei einigen Firmware-Aktualisierungen muss der Host nicht neu gestartet werden. In dem Fall wird die Firmware-Aktualisierung durchgeführt, ohne dass der Host in den Wartungsmodus wechselt.

Der Garantie- und Bestandsaufnahme-Zeitplan für alle vCenter wird nicht angewendet, wenn er unter „Dell Home > Überwachen > Job-Warteschlange > Garantie/ Bestandsaufnahmeverlauf > Zeitplan“ ausgewählt wird.

Ein Kunde wechselt zur Seite „Auftragswarteschlange“, wählt ein vCenter und die Schaltfläche „Zeitplan ändern“ aus. Wenn das Dialogfeld angezeigt wird, wird ein Kontrollkästchen angezeigt, dass zur Anwendung für alle registrierten vCenters auffordert. Wenn dies ausgewählt und auf „Anwenden“ geklickt wird, gilt die Einstellung nur für das ursprünglich ausgewählte vCenter und nicht für alle vCenter. Die Meldung „Für alle registrierten vCenter übernehmen“ wird nicht angewendet, wenn der Garantie- oder Bestandsaufnahmezeitplan von der Job-Warteschlange aus modifiziert wird.

Lösung: Verwenden Sie den Garantie- oder Bestandsaufnahme-Zeitplan in der Job-Warteschlange nur zum Modifizieren des ausgewählten vCenters.

Betroffene Versionen: 2.2 und 2.3

Warum wird das Installationsdatum als 31.12.1969 für einige Firmwareversionen auf der Firmware-Seite angezeigt?

Das im Web-Client angezeigte Datum wird als 31.12.1969 für einige Firmwares eines Hosts auf der Firmware-Seite angezeigt. Sollte kein Firmware-Installationsdatum zur Verfügung stehen, wird dieses alte Datum angezeigt.

Lösung: Wenn Sie dieses alte Datum für eine Firmware-Komponente sehen, ist das wirkliche Installationsdatum nicht verfügbar.

Betroffene Versionen: 2.2 und 2.3

Warum ist der globale Gehäuse-Funktionszustand immer noch funktionsfähig, wenn sich einige der Netzteil-Stati auf kritisch geändert haben?

Der globale Funktionszustand des Gehäuses bezogen auf die Stromversorgung basiert auf den Redundanzrichtlinien und ob die Stromversorgungsanforderungen des Gehäuses von den Netzteilen, die noch online und funktionstüchtig sind, erfüllt werden. Auch wenn einige der Netzteileinheiten über keinen Strom verfügen, werden die gesamten Anforderungen an die Stromversorgung des Gehäuses erfüllt. Daher ist der globale Funktionszustand des Gehäuses funktionsfähig. Weitere Informationen über die Stromversorgung und der Energieverwaltung finden Sie im Benutzerhandbuch der Dell PowerEdge M1000e Chassis Management Controller-Firmware.

Warum wird in der Ansicht „Prozessor“ auf der Seite „System-Überblick“ die Prozessor-Version als „Nicht verfügbar“ angezeigt?

Im Fall von Dell PowerEdge-Servern der 12. Generation und höher wird die Prozessor-Version in der Marken-Spalte angezeigt. Bei niedrigeren Generation wird die Prozessor-Version in der Versions-Spalte angezeigt.

Warum führt das wiederholte globale Aktualisieren zu einer Ausnahme im aktuellen Task-Fenster?

Wenn ein Kunde versucht wiederholt auf die Schaltfläche „Aktualisieren“ zu drücken, tritt möglicherweise eine Ausnahme in der VMware-Benutzeroberfläche auf.

Lösung: Der Benutzer sollte diese Fehlermeldung schließen und fortfahren.

Betroffene Versionen: 2.2 und 2.3

Warum ist die Web-Client-Benutzeroberfläche für einige der Dell-Bildschirme in IE 10 verzerrt?

In einigen Fällen, wenn ein Informationsdialogfeld angezeigt wird, sind die Daten im Hintergrund vollständig weiß und werden möglicherweise verzerrt dargestellt.

Lösung: Schließen Sie das Dialogfeld und der Bildschirm wird wieder normal.

Betroffene Versionen: 2.2 und 2.3

Die Verwendung von OpenManage Integration for VMware vCenter zum Aktualisieren einer Intel-Netzwerkkarte mit der Firmwareversion 13.5.2 wird nicht unterstützt.

Es gibt ein bekanntes Problem mit der 12. Generation der Dell PowerEdge-Server und einigen Intel-Netzwerkkarten mit der Firmwareversion 13.5.2. Das Aktualisieren einiger Intel-Netzwerkkartenmodelle mit dieser Firmwareversion schlägt fehl, wenn die Firmware-Aktualisierung mithilfe von Lifecycle Controller durchgeführt wird. Kunden, die diese Firmwareversion verwenden, müssen die Netzwerktreibersoftware mithilfe eines Betriebssystems aktualisieren. Wenn die Firmwareversion der Intel-Netzwerkkarte eine andere ist als 13.5.2, können Sie die Aktualisierung mithilfe von OpenManage Integration for VMware vCenter durchführen. Weitere Informationen finden Sie unter http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx.



ANMERKUNG: Hinweis: Wählen Sie bei der Anwendung einer Firmware-Aktualisierung vom Typ 1:n keine Intel-Netzwerkadapter der Version 13.5.2 aus. Anderenfalls schlägt die Aktualisierung fehl und die Aktualisierungsaufgabe für die verbleibenden Server wird gestoppt.

Selbst wenn mein Repository über Bundles für das ausgewählte 11G-System verfügt, zeigt die Firmware-Aktualisierung, dass ich über keine Bundles für eine Firmware-Aktualisierung verfüge, an.

Als ich im Sperrmodus einen Host zum Verbindungsprofil hinzugefügt habe, wurde eine Bestandsaufnahme gestartet, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt“ fehlschlug. Die Bestandsaufnahme sollte jedoch für einen Host im Sperrmodus funktionieren, oder?

Wenn Sie den Host in den Sperrmodus versetzen oder den Sperrmodus von einem Host entfernen, müssen Sie mindestens 30 Minuten warten, bevor Sie mit dem nächsten Vorgang in der Option „Wenn ich einen 11G-Host für eine Firmware-Aktualisierung auswähle“ durchführen können. Der Assistent zur Firmware-Aktualisierung zeigt keine Bundles an, selbst, wenn das Repository Bundles für das System bereitgestellt hat. Dies tritt ein, da der 11G-Host eventuell nicht dafür konfiguriert ist, dass OMSA Traps zu OpenManage Integration sendet.

Lösung: Stellen Sie sicher, dass der Host mit dem Host-Compliance-Bildschirm des OpenManage Integration Desktop-Clients kompatibel ist. Wenn sie nicht konform sind, verwenden Sie die Option „Host-Konformitätprobleme beheben“, um die Konformität herzustellen.

Betroffene Versionen: 2.2 und 2.3

Warum sehe ich das OpenManage Integration-Symbol im Web-Client-Ereignis, selbst wenn die Registrierung des Plug-ins im vCenter erfolgreich war?

Das OpenManage Integration-Symbol wird nicht auf dem Web-Client angezeigt, sofern der Web-Client-Service oder die Box nicht neu gestartet werden. Wenn ein Benutzer das OpenManage Integration for VMware vCenter-Gerät registriert, werden beide, der Desktop-Client sowie der Web-Client, registriert. Wenn ein Benutzer die Registrierung des Geräts aufhebt und danach dieselbe Version oder eine neuere Version des Geräts erneut registriert, werden zwar beide Clients

erfolgreich registriert, aber das Dell-Symbol erscheint eventuell nicht im Web-Client. Zur Behebung des Problems muss der Benutzer den Web-Client-Service auf dem vCenter-Server neu starten. Nur dann erscheint das Plug-in in der Benutzeroberfläche.

Lösung: Starten Sie den Web-Client-Service auf dem vCenter-Server neu.

Betroffene Versionen: 2.2 und 2.3

Ich erhalte eine Ausnahme, wenn ich auf „Beenden“ klicke, nachdem ich ein Verbindungsprofil durch den Web-Client bearbeitet habe. Warum?

Dies geschieht, wenn der vCenter-Server beim Gerät durch IP anstelle von FQDN registriert ist. Das Verbindungsprofil kann durch den Desktop-Client bearbeitet werden. Das erneute Registrieren des vCenter-Servers mit demselben Gerät löst das Problem nicht. Es ist ein neues Setup mit registriertem FQDN erforderlich.

Ich kann die Verbindungsprofile zu dem der Host gehört, bei der Erstellung/Bearbeitung eines Verbindungsprofils in der Web-GUI nicht sehen. Warum?

Dies geschieht, wenn der vCenter-Server bei dem Gerät durch IP, anstelle von FDQN registriert ist. Das erneute Registrieren des vCenter-Servers mit demselben Gerät löst das Problem nicht. Ein neues Setup mit einer Registrierung bei FDQN ist erforderlich.

Beim Bearbeiten eines Verbindungsprofils ist das ausgewählte Host-Fenster in der Web-Benutzeroberfläche leer. Warum?

Dies geschieht, wenn der vCenter-Server bei dem Gerät durch IP anstelle von FDQN registriert ist. Das Problem wird nicht duch das erneute Registrieren des vCenter-Servers bei demselben Gerät gelöst. Ein neues Setup mit einer Registrierung bei FDQN ist erforderlich.

Warum wird nach dem Anklicken des Firmware-Links eine Kommunikationsfehlermeldung angezeigt?

Wenn Sie eine langsame Netzwerkverbindung haben (9.600 Bit/s), erhalten Sie eventuell eine Kommunikationsfehlermeldung. Diese wird möglicherweise dann angezeigt, wenn Sie im vSphere-Client auf den Firmware-Link für die OpenManage Integration for VMware vCenter klicken. Dies geschieht, wenn das Zeitlimit für die Verbindung abläuft, während versucht wird, die Liste mit dem Softwarebestand abzurufen. Diese Zeitüberschreitung wird von Microsoft Internet Explorer initiiert. Bei den Versionen 9 und 10 von Microsoft Internet Explorer ist der Wert für die „Zeitüberschreitung beim Empfangen“ auf 10 Sekunden voreingestellt. Beheben Sie das Problem, indem Sie die folgenden Schritte durchführen.

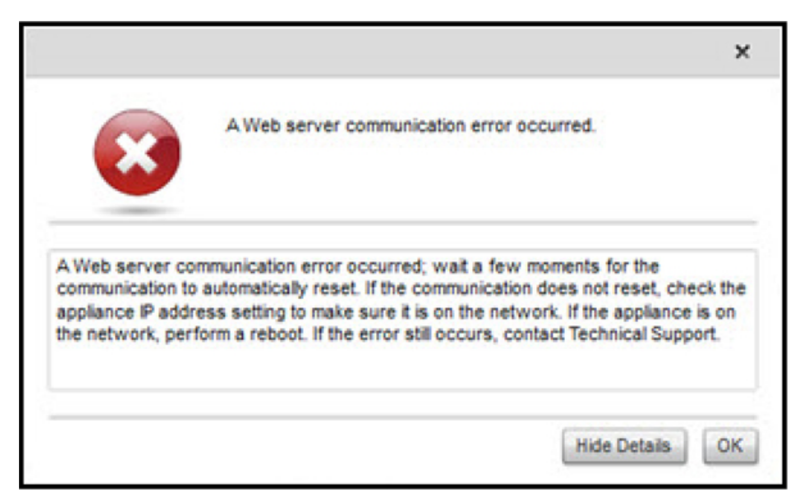


Abbildung 1. Firmware-Link-Kommunikationsfehler

1. Öffnen Sie den Microsoft- Registrierungs-Editor (Regedit).
2. Navigieren Sie zum folgenden Ort in der Registrierung:

   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Fügen Sie einen DWORD-Wert für die Zeitüberschreitung beim Empfangen (ReceiveTimeout) hinzu.
4. Setzen Sie den Wert auf 30 Sekunden (30.000) [Möglicherweise muss der Wert für Ihre Umgebung höher eingestellt werden].
5. Beenden Sie Regedit.
6. Starten Sie Internet Explorer neu.

    **ANMERKUNG:** Es genügt nicht, ein neues Internet Explorer-Fenster zu öffnen. Sie müssen den Internet Explorer-Browser komplett neu starten.

Welche Generation von Dell Servern kann OpenManage Integration for VMware vCenter für SNMP-Traps konfigurieren und unterstützen?

OpenManage Integration for VMware vCenter unterstützt OMSA-SNMP-Traps auf Servern vor der 12. Generation und iDRAC-Traps auf Servern der 12. Generation.

Welche vCenter im verknüpften Modus werden von OpenManage Integration for VMware vCenter verwaltet?

OpenManage Integration for VMware vCenter verwaltet ausschließlich registrierte vCenter im verknüpften Modus.

Unterstützt OpenManage Integration for VMware vCenter vCenter im verknüpften Modus?

Ja, OpenManage Integration for VMware vCenter unterstützt bis zu 10 vCenters im verknüpften Modus. Weitere Informationen über die Funktionsweise von OpenManage Integration for VMware vCenter im verknüpften Modus finden Sie im Whitepaper *Dell Management Plug-in for VMware vCenter: die Arbeit im verknüpften Modus* auf www.Dell.com.

Was sind die erforderlichen Schnittstelleneinstellungen für das OpenManage Integration for VMware vCenter?



ANMERKUNG: HINWEIS: Wenn Sie den OMSA-Agenten über den Link *Probleme auf nicht-konformen vSphere-Hosts beheben* bereitstellen, der im Fenster „Übereinstimmung" in OpenManage Integration for VMware vCenter angezeigt wird, startet das OpenManage Integration for VMware vCenter den httpClient-Dienst, aktiviert Port 8080 auf Versionen nach ESXi 5.0, um OMSA VIB herunterzuladen und zu installieren. Sobald die OMSA-Installation abgeschlossen ist, wird der Dienst automatisch angehalten, und die Schnittstelle wird geschlossen.

Verwenden Sie diese Schnittstelleneinstellungen für das OpenManage Integration for VMware vCenter.

Tabelle 4. Schnittstelle virtueller Geräte

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
21	FTP	TCP	Keine	Ausgang	FTP-Befehls-Client	Nein
53	DNS	TCP	Keine	Ausgang	DNS-Client	Nein
80	HTTP	TCP	Keine	Ausgang	Dell Online-Datenzugriff	Nein
80	HTTP	TCP	Keine	Eingang	Verwaltungskonsole	Nein
162	SNMP-Agent	UDP	Keine	Eingang	SNMP-Agent (Server)	Nein
11620	SNMP-Agent	UDP	Keine	Eingang	SNMP-Agent (Server)	Nein
443	HTTPS	TCP	128–Bit	Eingang	HTTPS-Server	No
443	WSMAN	TCP	128–Bit	Ein/Aus	iDRAC/OMSA-Kommunikation	Nein
4433	HTTPS	TCP	128–Bit	Eingang	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
11620	SNMP-Agent	UDP	Keine	OM	SNMP-Agent (Server)	Nein

Tabelle 5. Verwaltungsknoten

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
162, 11620	SNMP	UDP	Keine	Ausgang	Hardware-Ereignisse	Nein
443	WSMAN	TCP	128–Bit	Eingang	iDRAC/OMSA-Kommunikation	Nein

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
4433	HTTPS	TCP	128–Bit	Ausgang	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
443	HTTPS	TCP	128–Bit	Eingang	HTTPS-Server	Nein
8080	HTTP	TCP		Eingang	HTTP-Server; lädt den OMSA VIB herunter und behebt nicht konforme vSphere-Hosts	Nein
50	RMCP	UDP/TCP	128–Bit	Ausgang	Remote Mail Check Protocol	Nein
51	IMP	UDP/TCP	k.A.	k.A.	IMP Logical Address Maintenance	Nein
5353	mDNS	UDP/TCP		Alle	Multicast DNS	Nein
631	IPP	UDP/TCP	None	Ausgang	Internet Printing Protocol (IPP)	Nein
69	TFTP	UDP	128–Bit	Alle	Trivial File Transfer (Einfache Dateiübertragung)	Nein
111	NFS	UDP/TCP	128–Bit	Eingang	SUN Remote Procedure Call (Portmap)	Nein
68	BOOTP	UDP	Keine	Ausgang	Bootstrap Protocol Client	Nein

Welche Mindestanforderungen bestehen für die erfolgreiche Installation und den erfolgreichen Betrieb des virtuellen Geräts?

Die folgenden Einstellungen stellen die Mindestanforderungen für das Gerät dar:

- Physischer RAM: 3 GB.
- Reservierter Arbeitsspeicher: 1 GB

  ANMERKUNG: Für optimale Leistung empfiehlt Dell 3 GB.

- Festplatte: 32,5 GB.
- CPU: 2 virtuelle CPUs.

Warum werden keine Einzelheiten meiner neuen iDRAC-Version auf der Seite der vCenter Hosts & Cluster angezeigt?

Aktualisieren Sie nach der erfolgreichen Fertigstellung einer Firmware-Aktualisierungsaufgabe im Fensterbereich der jüngsten Aufgaben des vSphere Web-Clients die Firmware-Aktualisierungsseite und überprüfen Sie die Firmware-Versionen. Wenn auf der Seite die alten Versionen angezeigt werden, navigieren Sie zur Host-Konformitätsseite in OpenManage Integration for VMware vCenter und prüfen Sie den CISOR-Status dieses Hosts. Wenn CISOR nicht aktiviert ist, aktivieren Sie CISOR und starten Sie den Host neu. Wenn CISOR bereits aktiviert war, melden Sie sich an der iDRAC-Konsole an, setzen Sie den iDRAC zurück, warten Sie einige Minuten und aktualisieren Sie dann die Firmware-Aktualisierungsseite im vSphere-Web-Client.



ANMERKUNG: Die Host-Übereinstimmung ist nicht im Web-Client verfügbar und es muss die Host-Übereinstimmungsfunktion des vSphere Desktop-Client verwendet werden.

Wie teste ich Ereigniseinstellungen mithilfe des OMSA, um einen Temperaturfehler an der Hardware zu simulieren?

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass die Ereignisse korrekt funktionieren:

1. Navigieren Sie in der OMSA-Benutzeroberfläche zu **Warnungsverwaltung** → **Plattformereignisse**.
2. Aktivieren Sie das Kontrollkästchen **Plattformereignisfilter-Warnungen aktivieren**.
3. Führen Sie einen Bildlauf bis ganz nach unten durch, und klicken Sie auf **Änderungen anwenden**.
4. Um sicherzugehen, dass ein bestimmtes Ereignis aktiviert ist, wie z. B. Temperaturwarnung, wählen Sie aus der Struktur auf der linken Seite die Option **Hauptsystemgehäuse aus**.
5. Wählen Sie unter **Hauptsystemgehäuse Temperaturen** aus.
6. Wählen Sie die Registerkarte **Warnungsverwaltung** und anschließend **Temperatursondenwarnung** aus.
7. Aktivieren Sie das Kontrollkästchen **Broadcast-Übertragung einer Meldung**, und wählen Sie **Änderungen anwenden** aus.
8. Um das Temperaturwarnereignis auszulösen, wählen Sie in der Strukturansicht auf der linken Seite die Option **Hauptsystemgehäuse** aus.
9. Wählen Sie unter **Hauptsystemgehäuse** die Option **Temperaturen** aus.
10. Wählen Sie den Link **Umgebungstemp. der Systemplatine** und dann die Options-Schaltfläche **Auf Werte setzen** aus.
11. Stellen Sie die Option **Maximaler Warnungsschwellenwert** auf einen Wert niedriger als der aktuelle angegebene Messwert ein. Wenn der aktuelle Messwert beispielsweise 27 lautet, stellen Sie den Schwellenwert auf **25**.
12. Wählen Sie **Änderungen anwenden** aus, woraufhin das Temperaturwarnungsereignis generiert wird. Wenn Sie ein weiteres Ereignis auslösen möchten, müssen Sie die ursprünglichen Einstellungen mithilfe der gleichen Option **Auf Werte setzen** wiederherstellen. Die Ereignisse werden als Warnungen generiert und dann auf einen normalen Zustand gesetzt. Wenn alle Vorgänge ordnungsgemäß funktionieren, wechseln Sie zur Ansicht **vCenter-Tasks & -Ereignisse**. Darin sollte keine Temperatursondenwarnung angezeigt werden.

   ANMERKUNG: Es gibt einen Filter für doppelte Ereignisse. Wenn Sie versuchen, dasselbe Ereignis zu oft hintereinander auszulösen, erhalten Sie nur ein Ereignis. Um alle Ereignisse anzuzeigen, müssen Sie mindestens 30 Sekunden zwischen dem Auslösen der Ereignisse warten.

Ich habe den OMSA-Agenten auf einem Dell-Hostsystem installiert, es wird jedoch weiterhin eine Fehlermeldung angezeigt, dass OMSA nicht installiert ist. Wie muss ich vorgehen?

Um dieses Problem auf einem Server der 11. Generation zu beheben:

1. Installieren Sie den **OMSA** mit der Komponente **Remote-Aktivierung** auf dem Hostsystem.
2. Wenn Sie den OMSA über die Befehlszeile installieren, müssen Sie die **Option -c** angeben. Wenn der OMSA bereits installiert ist, installieren Sie ihn erneut mit der Option -c, und starten Sie den Dienst neu:

   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

   Bei einem ESXi-Host müssen Sie **OMSA-VIB** mithilfe des **VMware-Remote-CLI-Tool** installieren, und das System neu starten.

Unterstützt das OpenManage Integration for VMware vCenter ESX/ESXI mit aktiviertem Sperrmodus?

Ja. Der Sperrmodus wird in dieser Version auf den Hosts ESXi 4.1 und höher unterstützt.

Nach einem Neustart tritt bei der Bestandsaufnahme auf den Hosts ESXi 4.0 Update2 und ESXi Update3 im Sperrmodus ein Fehler auf.

Für den Sperrmodus ist ESXi 4.1 oder höher erforderlich. Wenn Sie eine frühere ESXi-Version verwenden und ein Host aus einem beliebigen Grund im Sperrmodus neu gestartet wird, treten bei der Bestandsaufnahme auch weiterhin Fehler auf, sofern Sie nach einem Neustart nicht die folgenden Schritte auf dem Host ausführen.

Schritte für die Problemumgehung bei ESXi 4.0 Update2 und Update3:

1. Klicken Sie unter **vSphere Web-Client** auf die Option **Hosts und Cluster**, wählen Sie dann im linken Fenster den **Host** aus, und klicken Sie anschließend auf die Registerkarte **Konfiguration**.
2. Klicken Sie im linken Fenster unter **Software** auf **Sicherheitsprofil**.
3. Führen Sie einen Bildlauf bis zu **Sperrmodus** durch, und klicken Sie dann auf **Bearbeiten**.
4. Löschen Sie zum Deaktivieren des Sperrmodus im Dialogfeld **Sperrmodus** das Häkchen im Kontrollkästchen **Aktivieren**, und klicken Sie dann auf **OK**.
5. Melden Sie sich bei der Hostkonsole an, und wählen Sie **Verwaltungs-Agenten neu starten** aus. Drücken Sie die **<EINGABETASTE>** und zum Bestätigen die Taste **<F11>**.
6. Wiederholen Sie zum Aktivieren des Sperrmodus die Schritte 1 bis 4, wählen Sie jedoch diesmal das Kontrollkästchen **Aktivieren** aus, und klicken Sie anschließend auf **OK**.

Beim Verwenden des Sperrmodus ist ein Fehler aufgetreten.

Als ich im Sperrmodus einen Host zum Verbindungsprofil hinzugefügt habe, wurde eine Bestandsaufnahme gestartet, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt.“ fehlschlug. Die Bestandsaufnahme sollte jedoch für einen Host im Sperrmodus funktionieren, oder?

Wenn Sie den Host in den Sperrmodus versetzen oder den Sperrmodus des Hosts entfernen, müssen Sie 30 Minuten warten, bevor Sie den nächsten Vorgang auf dem OpenManage Integration for VMware vCenter ausführen.

Welche Einstellung sollte ich für UserVars.CIMoeMProviderEnable mit ESXi 4.1 U1 verwenden?

Stellen Sie **UserVars.CIMoemProviderEnabled** auf 1 ein.

Ich habe ein Hardware-Profil mithilfe eines Referenzservers erstellt, es ist jedoch fehlerhaft. Was kann ich tun?

Überprüfen Sie, ob die empfohlenen Mindestversionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS installiert sind.

Um sicherzustellen, dass die vom Referenzserver abgerufenen Daten aktuell sind, müssen Sie die Option **Systembestandsaufnahme beim Neustart sammeln (CSIOR)** aktivieren und den Referenzserver vor der Datenextrahierung neu starten.

Ich möchte ESX/ESXi auf einem Blade-Server bereitstellen, dabei tritt jedoch ein Fehler auf. Wie muss ich vorgehen?

1. Stellen Sie sicher, dass der **ISO-Speicherort (NFS-Pfad)** und die **Stagingordnerpfade** stimmen.
2. Achten Sie darauf, dass sich die während der Zuweisung der Serveridentität ausgewählte **NIC** auf dem gleichen Netzwerk wie das virtuelle Gerät befindet.
3. Falls Sie mit einer **statischen IP-Adresse** arbeiten, müssen Sie sich vergewissern, dass die angegebenen Netzwerkinformationen (einschließlich Subnetzmaske und Standard-Gateway) stimmen. Stellen Sie darüber hinaus sicher, dass die IP-Adresse nicht bereits einem anderen Netzwerk zugewiesen ist.
4. Achten Sie darauf, dass mindestens eine **virtuelle Festplatte** vom System erkannt wird. ESXi kann auch auf einer internen RIPS SD-Karte installiert werden.

Warum schlagen meine Hypervisor-Bereitstellungen auf meinen Dell PowerEdge R210-II-Maschinen fehl?

Ein Zeitüberschreitungsproblem auf Dell PowerEdge R210-II-Maschinen verursacht eine Hypervisor-Bereitstellungs-Fehlermeldung, da das BIOS nicht vom zugehörigen ISO starten kann. Installieren Sie den Hypervisor manuell auf der Maschine, um dieses Problem zu beheben.

Warum werden automatisch erkannte Systeme im Bereitstellungsassistenten ohne Modellinformationen angezeigt?

Meist bedeutet dies, dass die auf dem System installierte Firmware-Version nicht die empfohlenen Mindestanforderungen erfüllt. In einigen Fällen wurde möglicherweise eine Firmware-Aktualisierung nicht auf dem System registriert. Durch einen Kaltstart des Systems oder erneutes Einsetzen des Blades wird dieses Problem behoben. Das neu aktivierte Konto auf dem iDRAC muss deaktiviert und die automatische Erkennung neu initiiert werden, um Modellinformationen und NIC-Informationen für das OpenManage Integration for VMware vCenter bereitzustellen.

Die NFS-Freigabe wurde mit dem ESX/ESXI-ISO eingerichtet, die Bereitstellung schlägt jedoch mit Fehlern beim Laden des Freigabepfads fehl.

Gehen Sie folgendermaßen vor, um die Lösung zu finden:

1. Stellen Sie sicher, dass der iDRAC einen Ping-Befehl an das Gerät senden kann.
2. Stellen Sie außerdem sicher, dass Ihr Netzwerk nicht zu langsam ist.

3. Stellen Sie sicher, dass die Anschlüsse: 2049, 4001 – 4004 offen sind und die Firewall entsprechend eingestellt ist.

Wie kann ich die Entfernung des virtuellen Geräts erzwingen?

1. Wechseln Sie zu **https://<vCenter_Server-IP-Adresse>/mob**
2. Geben Sie die VMware vCenter Administrator-Anmeldeinformationen ein.
3. Klicken Sie auf **Inhalt** .
4. Klicken Sie auf **ExtensionManager**.
5. Klicken Sie auf **UnregisterExtension**.
6. Geben Sie den Erweiterungsschlüssel zur Deregistrierung von com.dell.plugin.openManage_integration_for_VMware_vCenter ein und klicken Sie anschließend auf **Methode aufrufen**.
7. Geben Sie den Erweiterungsschlüssel zur Deregistrierung von com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient ein und klicken Sie anschließend auf **Methode aufrufen**.
8. Schalten Sie das OpenManage Integration for VMware vCenter im vSphere-Web-Client aus und löschen Sie es. Der Schlüssel zum Aufheben der Registrierung muss für den Web-Client sein.

Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt.

Wenn Sie einen Monitor mit niedriger Auflösung verwenden, wird das Feld Verschlüsselungskennwort nicht im Fenster JETZT SICHERN angezeigt. Sie müssen auf der Seite einen Bildlauf nach unten durchführen, um das Verschlüsselungskennwort einzugeben.

Im vSphere-Web-Client gibt das Klicken auf das Dell Server Management-Portlet oder das Dell-Symbol einen 404-Fehler aus.

Überprüfen Sie, ob das Gerät ausgeführt wird. Starten Sie es ggf. vom vSphere-Client neu. Warten Sie einige Minuten, bis der Webdienst des virtuellen Geräts gestartet wurde, und aktualisieren Sie die Seite. Wenn der Fehler weiterhin auftritt, versuchen Sie das Gerät mithilfe der IP-Adresse oder eines vollqualifizierten Domänennamens von einer Befehlszeile aus zu pingen. Wenn der Fehler durch den Ping-Befehl nicht behoben wird, überprüfen Sie, ob Ihre Netzwerkeinstellungen korrekt sind.

Bei meiner Firmware-Aktualisierung ist ein Fehler aufgetreten. Wie muss ich vorgehen?

Prüfen Sie in den Protokollen des virtuellen Geräts, ob bei der Aufgabe ein Timeout aufgetreten ist. In diesem Fall muss der iDRAC durch einen kalten Neustart zurückgesetzt werden. Nachdem das System wieder läuft, überprüfen Sie entweder durch Ausführen einer Bestandsaufnahme oder über die Registerkarte „Firmware“, ob die Aktualisierung erfolgreich war.

Meine vCenter-Registrierung ist fehlgeschlagen. Was kann ich tun?

Die vCenter-Registrierung kann aufgrund von Kommunikationsproblemen fehlschlagen. Als Lösung für diese Probleme kann eine statische IP-Adresse verwendet werden. Um eine statische IP-Adresse zu verwenden, wählen Sie auf der Registerkarte „Konsole“ des OpenManage Integration for VMware vCenter die Option **Netzwerk konfigurieren** → **Geräte bearbeiten** aus, und geben Sie das richtige **Gateway** und den richtigen **FQDN** (vollqualifizierter Domänenname) ein. Geben Sie dann unter „DNS-Konfig bearbeiten“ den Namen des DNS-Servers an.



ANMERKUNG: Stellen Sie sicher, dass das virtuelle Gerät den eingegebenen DNS-Server auflösen kann.

Die Leistung ist, während des Tests der Anmeldeinformationen des Verbindungsprofils extrem langsam und die Anwendung reagiert nicht.

Der iDRAC auf einem Server hat nur einen Benutzer (z. B. nur *Stammbenutzer*) und der Benutzer ist deaktiviert oder alle Benutzer befinden sich in einem deaktivierten Zustand. Bei der Kommunikation mit einem Server in einem deaktivierten Zustand kommt es zu Verzögerungen. Um dieses Problem zu beheben, können Sie entweder den deaktivierten Zustand des Servers aufheben oder den iDRAC auf dem Server zurücksetzen, um den Stammbenutzer wieder auf die Standardeinstellung zu aktivieren.

Gehen Sie wie nachfolgend beschrieben vor, um das Problem mit einem Server in einem deaktivierten Zustand zu beheben:

1. Öffnen Sie die Konsole „Chassis Management Controller“, und wählen Sie den deaktivierten Server aus.
2. Um die iDRAC-Konsole automatisch zu öffnen, klicken Sie auf **iDRAC-GUI starten**.
3. Navigieren Sie zur Benutzerliste in der iDRAC-Konsole, und wählen Sie eine der folgenden Optionen:
   - iDRAC 6: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Netzwerk/Sicherheit** → **Benutzer**.
   - iDRAC 7: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Benutzer**.
   - iDRAC 8: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Benutzer**.
4. Um die Einstellungen zu bearbeiten, klicken Sie in der Spalte „Benutzer-ID“ auf den Link für den Admin-(Stamm-)Benutzer..
5. Klicken Sie auf **Benutzer konfigurieren** und dann auf **Weiter**.
6. Aktivieren Sie auf der Seite „Benutzerkonfiguration“ für den ausgewählten Benutzer das Kontrollkästchen neben „Benutzer aktivieren“, und klicken Sie dann auf **Anwenden**.

Unterstützt OpenManage Integration for VMware vCenter das VMware vCenter Server-Gerät?

Ja, OpenManage Integration for VMware vCenter v2.1 unterstützt das VMware vCenter Server-Gerät.

Unterstützt OpenManage Integration for VMware vCenter den vSphere-Web-Client?

Ja, OpenManage Integration for VMware vCenter unterstützt den VMware vSphere-Web-Client.

Warum ist meine Firmware-Version immer noch nicht aktualisiert, wenn ich die Firmware-Aktualisierung mit der Option "Beim nächsten Neustart anwenden" ausgeführt habe und das System neu gestartet wurde?

Um die Firmware zu aktualisieren, führen SIe die Bestandsaufnahme auf dem Host aus, wenn der Neustart abgeschlossen ist. In einigen Fällen, in denen das Neustartereignis das Gerät nicht erreicht, wird die Bestandsliste nicht automatisch gestartet. In dieser Situation müssen Sie die Bestandsaufnahme manuell neu ausführen, um die aktualisierten Firmware-Versionen zu ermitteln.

Warum wird der Host weiterhin unter dem Gehäuse angezeigt, selbst wenn Sie den Host aus der vCenter-Struktur entfernt haben?

Die Hosts unter dem Gehäuse werden als Teil der Gehäuse-Bestandsaufnahme identifiziert. Nach einer erfolgreichen Gehäuse-Bestandsaufnahme wird die Hostliste unter dem Gehäuse aktualisiert. Daher wird der Host bis zur Ausführung der nächsten Gehäuse-Bestandsaufnahme immer noch unter dem Gehäuse angezeigt, auch wenn der Host aus der vCenter-Struktur entfernt wurde.

Warum wird der Aktualisierungs-Repository-Pfad in der Administration Console nicht auf den Standard-Pfad nach dem Zurücksetzen des Geräts auf die werkseitigen Einstellungen eingestellt?

Nachdem Sie das Gerät zurückgesetzt haben, gehen Sie auf die Administration Console und klicken Sie auf der linken Seite auf **GERÄTEVERWALTUNG**. Auf der Seite **Geräteeinstellungen** ist der **Aktualisierungs-Repository-Pfad** nicht auf die Standardeinstellungen zurückgesetzt.

Lösung: Kopieren Sie in der Administration Console manuell den Pfad im Feld **Standard-Aktualisierungs-Repository** in das Feld **Repository-Aktualisierungspfad**.

Warum werden die Alarm-Einstellungen nicht nach der Sicherung und Wiederherstellung von OpenManage Integration for VMware vCenter wiederhergestellt?

Das Wiederherstellen der OpenManage Integration for VMware vCenter-Gerätesicherung stellt nicht alle Alarm-Einstellungen wieder her. Es werden jedoch in der OpenManage Integration for VMware-GUI im Feld **Ereignisse und Alarme** die wiederhergestellten Einstellungen angezeigt.

Lösung: Ändern Sie in OpenManage Integration for VMware-GUI auf der Registerkarte **Verwalten** → **Einstellungen** manuell die Einstellungen für **Ereignisse und Alarme**.

Probleme bei der Bare-Metal-Bereitstellung

Dieser Abschnitt behandelt Probleme während des Bereitstellungsvorgangs. Die v 2.1 unterstützt nicht die Bereitstellung vom Web-Client aus, sondern nur unter Verwendung des vSphere Desktop-Clients.

Voraussetzungen für Auto-Ermittlung und Handshake

- Bevor Sie Auto-Ermittlung und Handshake ausführen können, müssen Sie sicherstellen, dass die Versionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS die Mindestempfehlungen erfüllen.
- CSIOR muss mindestens einmal auf dem System oder iDRAC ausgeführt worden sein.

Hardware-Konfigurationsfehler

- Achten Sie vor der Initialisierung einer Bereitstellungsaufgabe darauf, dass das System CSIOR abgeschlossen hat und nicht gerade neu gestartet wird.
- Es wird dringend empfohlen, die BIOS-Konfiguration im Klonmodus auszuführen, sodass der Referenzserver ein identisches System ist.
- Manche Controller erlauben keine Erstellung von RAID 0 mit nur einem Laufwerk. Diese Funktion wird nur auf High-End-Controllern unterstützt und die Anwendung solcher Hardwareprofile kann zu Ausfällen führen.

Kontaktaufnahme mit Dell



ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

1. Rufen Sie die Website **dell.com/support** auf.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region in der Drop-Down-Liste **Land oder Region auswählen** am unteren Seitenrand aus.

4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

Weitere Hilfe für diese Software

Dell-Virtualisierungsdokumentation können Sie unter folgender Adresse anzeigen oder herunterladen: **http://support.dell.com/support/edocs/software/eslvmwre/**. Häufig gestellte Fragen zum Dell vCenter-Plugin finden Sie unter **http://i.dell.com/sites/content/business/solutions/virtualization/en/Docu ments/dell-management-plugin-vmware-vcenter-faq.pdf**

Verwandte Informationen zum Dell Management Plug-in for VMware vCenter

- Anzeigen oder Herunterladen von VMware vSphere 4d für Dell PowerEdge-Server
  http://en.community.dell.com/techcenter/virtualization/w/wiki/vmware.aspx
- Anzeigen oder Herunterladen von Dell-Serverdokumentation für PowerEdge™-Server unter:
  http://support.dell.com/support/systemsinfo/documentation.aspx?c= us&l=en&s=gen&~subcat=88&~cat=12
- Dokumentation zum Dell OpenManage-Systemadministrator
  http://support.dell.com/support/systemsinfo/documentation.aspx?c= us&l=en&s=gen&~subcat=108&~cat=6
- Dokumentation zum Dell Lifecycle-Controller
  http://support.dell.com/support/edocs/software/smusc/smlc/

43

Ereignisse im Zusammenhang mit der Virtualisierung

Die folgende Tabelle enthält die kritischen und Warnungsereignisse im Zusammenhang mit der Virtualisierung, einschließlich Name des Ereignisses, Beschreibung und Schweregrad.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Stromsensor hat einen Warnungswert erkannt	Ein Stromsensor im angegebenen System hat seinen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell – Stromsensor hat einen Fehlerwert erkannt	Ein Stromsensor im angegebenen System hat seinen Fehlerschwellenwert überschritten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Stromsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Stromsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Redundanz wiederhergestellt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Redundanz beeinträchtigt	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten der Redundanzeinheit fehlgeschlagen, die Einheit aber dennoch redundant ist.	Warnung	Keine Maßnahme
Dell – Redundanz verloren	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten in der Redundanzeinheit getrennt wurde, fehlerhaft oder nicht vorhanden ist.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Netzteil auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme

Dell – Netzteil hat eine Warnung erkannt	Der Sensormesswert eines Netzteils im angegebenen System hat einen benutzerdefinierbaren Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell – Netzteil hat einen Fehler erkannt	Ein Netzteil wurde abgetrennt oder ist fehlerhaft.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Netzteilsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Netzteilsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Warnung über Status des Speichergeräts	Die Korrekturrate eines Speichergeräts hat einen akzeptierbaren Wert überschritten.	Warnung	Keine Maßnahme
Dell – Speichergerätfehler	Die Korrekturrate eines Speichergeräts hat einen akzeptierbaren Wert überschritten, eine Speicher-Spare-Bank wurde aktiviert oder es ist ein Multibit-ECC-Fehler aufgetreten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Lüftergehäuse in das System eingesetzt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Lüftergehäuse aus dem System entfernt	Ein Lüftergehäuse wurde aus dem angegebenen System entfernt.	Warnung	Keine Maßnahme
Dell – Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt	Ein Lüftergehäuse wurde für eine vom Benutzer festgelegte Zeitdauer aus dem angegebenen System entfernt.	Fehler	Keine Maßnahme
Dell – Lüftergehäusesensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Lüftergehäusesensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Netzstrom wurde wiederhergestellt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme

Dell – Warnung über verloren gegangenen Netzstrom	Ein Netzkabel hat seine Leistung verloren, die Redundanz ist jedoch ausreichend, um dies als Warnung zu klassifizieren.	Warnung	Keine Maßnahme
Dell – Ein Netzkabel hat seine Leistung verloren	Ein Netzkabel hat seine Leistung verloren und aufgrund fehlender Redundanz muss dies als Fehler klassifiziert werden.	Fehler	Keine Maßnahme
Dell – Prozessorsensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Prozessorsensor hat einen Warnungswert erkannt	Ein Prozessorsensor im angegebenen System befindet sich in einem gedrosselten Zustand.	Warnung	Keine Maßnahme
Dell – Prozessorsensor hat einen Fehlerwert erkannt	Ein Prozessorsensor im angegebenen System ist deaktiviert oder bei ihm ist ein Konfigurationsfehler bzw. ein thermischer Auslöser aufgetreten.	Fehler	Keine Maßnahme
Dell – Prozessorsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Prozessorsensor im angegebenen System ist fehlerhaft.	Fehler	Keine Maßnahme
Dell – Gerätekonfigurationsfehler	Für ein austauschbares Gerät im angegebenen System wurde ein Konfigurationsfehler erkannt.	Fehler	Keine Maßnahme
Dell – Batteriesensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Batteriesensor hat einen Warnungswert erkannt	Ein Batteriesensor im festgelegten System hat erkannt, dass sich ein Akku im vorhersehbaren Fehlerzustand befindet.	Warnung	Keine Maßnahme
Dell – Batteriesensor hat einen Fehlerwert erkannt	Ein Batteriesensor im festgelegten System hat erkannt, dass eine Batterie fehlerhaft ist.	Fehler	Keine Maßnahme
Dell – Batteriesensor hat einen nicht	Ein Batteriesensor im festgelegten System hat	Fehler	Keine Maßnahme

wiederherstellbaren Wert erkannt	erkannt, dass eine Batterie fehlerhaft ist.		
Dell – Temperaturbedingtes Herunterfahren wurde initiiert	Diese Meldung wird generiert, wenn ein System so konfiguriert wurde, dass es bei einem Fehlerereignis temperaturbedingt herunterfährt. Wenn der Messwert eines Temperatursensors den Fehlerschwellenwert überschreitet, für den das System konfiguriert wurde, fährt das Betriebssystem herunter und das System wird ausgeschaltet. Bei bestimmten Systemen kann dieses Ereignis auch initiiert werden, wenn ein Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt wird.	Fehler	Keine Maßnahme
Dell – Temperatursensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Temperatursensor hat einen Warnungswert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine, der CPU oder dem Festplattenträger im angegebenen System ermittelte ein Überschreiten des Warnungsschwellenwerts.	Warnung	Keine Maßnahme
Dell – Temperatursensor hat einen Fehlerwert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System ermittelte ein Überschreiten des Fehlerschwellenwerts.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Temperatursensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System erkannte einen Fehler, der	Fehler	Keine Maßnahme

	nicht behoben werden kann.		
Dell – Lüftersensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Lüftersensor hat einen Warnungswert erkannt	Ein Lüftersensormesswert in Host <x> hat einen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell – Lüftersensor hat einen Fehlerwert erkannt	Ein Lüftersensor im angegebenen System hat den Ausfall eines Lüfters oder mehrerer Lüfter erkannt.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Lüftersensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Lüftersensor hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Spannungssensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Spannungssensor hat einen Warnungswert erkannt	Ein Spannungssensor im angegebenen System hat seinen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell – Spannungssensor hat einen Fehlerwert erkannt	Ein Spannungssensor im angegebenen System hat seinen Fehlerschwellenwert überschritten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Spannungssensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Spannungssensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Stromsensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Speicher: Fehler bei der Speicherverwaltung	Die Speicherverwaltung hat einen geräteunabhängigen Fehlerzustand erkannt.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Controller-Warnung	Ein Teil der physische Festplatte ist beschädigt.	Warnung	Keine Maßnahme
Dell – Speicher: Controller-Fehler	Ein Teil der physische Festplatte ist beschädigt.	Fehler	Setzen Sie das System in den Wartungsmodus.

Dell – Speicher: Kanal-Fehler	Fehler beim Kanal.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Gehäuse-Hardware-Information	Information zur Gehäuse-Hardware.	Info	Keine Maßnahme
Dell – Speicher: Gehäuse-Hardware-Warnung	Warnung bezüglich Gehäuse-Hardware.	Warnung	Keine Maßnahme
Dell – Speicher: Gehäuse-Hardware-Fehler	Fehler der Gehäuse-Hardware.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Array-Festplattenfehler	Fehler der Array-Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: EMM-Fehler	EMM-Fehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Netzteilfehler	Netzteilfehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondenwarnung	Temperatursondenwarnung der physischen Festplatte: zu kalt oder zu heiß.	Warnung	Keine Maßnahme
Dell – Speicher: Temperatursondenfehler	Temperatursondenfehler der physischen Festplatte: zu kalt oder zu heiß.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Lüfterfehler	Lüfterfehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Batteriewarnung	Batteriewarnung.	Warnung	Keine Maßnahme
Dell – Speicher: Warnung: Virtuelle Festplatte wurde herabgesetzt	Warnung zur Herabsetzung einer virtuellen Festplatte.	Warnung	Keine Maßnahme
Dell – Speicher: Fehler: Virtuelle Festplatte wurde herabgesetzt	Fehler zur Herabsetzung einer virtuellen Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondeninformation	Informationen zur Temperatursonde	Info	Keine Maßnahme
Dell – Speicher: Array-Festplattenwarnung	Warnung zur Array-Festplatte.	Warnung	Keine Maßnahme
Dell – Speicher: Array-Festplatteninformation	Informationen zur Array-Festplatte.	Info	Keine Maßnahme
Dell – Speicher: Netzteilwarnung	Netzteilwarnung.	Warnung	Keine Maßnahme



Sicherheitsrollen und Berechtigungen

OpenManage Integration for VMware vCenterspeichert Benutzeranmeldeinformationen in einem verschlüsselten Format. Es liefert keine Kennwörter an Clientanwendungen, um nicht ordnungsgemäße Anforderungen zu vermeiden, die zu Problemen führen könnten. Die Datenbanksicherungen werden mithilfe benutzerdefinierter Sicherheitsausdrücke vollständig verschlüsselt, so dass die Daten nicht missbräuchlich verwendet werden können.

Standardmäßig verfügen Benutzer in der Gruppe der Administratoren über alle Berechtigungen. Administratoren können alle Funktionen der OpenManage Integration for VMware vCenter im VMware vCenter verwenden. Wenn Sie möchten, dass ein Nicht-Admin-Benutzer das Produkt verwaltet, dann erstellen Sie eine Rolle, die beide Dell-Rollen enthält, weisen Sie dann in der Bestandsliste auf dem root/übergeordneten (top)-Knoten eine Berechtigung zu und propagieren Sie Berechtigungen nach Bedarf auf die untergeordneten (child)-Knoten, für die Sie dem Benutzer Zugriff gewähren wollen. Zum Beispiel: Wenn Sie möchten, dass ein Benutzer nur Cluster A verwaltet, dann behalten Sie die Berechtigungen für Cluster A bei und entfernen Sie die Berechtigungen der anderen Cluster.



Datenintegrität

Die Kommunikation zwischen OpenManage Integration for VMware vCenter der Verwaltungskonsole und vCenter erfolgt über SSL/HTTPS. Das OpenManage Integration for VMware vCenter generiert ein SSL-Zertifikat für die vertrauenswürdige Kommunikation zwischen vCenter und der Appliance. Weiterhin wird das Serverzertifikat des vCenters vor der Kommunikation und der Registrierung des OpenManage Integration for VMware vCenterüberprüft und vertraut. Die OpenManage Integration for VMware vCenter Registerkarte „Konsole" (im VMware vCenter) verwendet Sicherheitsvorgänge zum Verhindern von inkorrekten Anfragen, während die Schlüssel zwischen der Verwaltungskonsole und dem Back-End-Service übertragen werden. Diese Art der Sicherheit führt dazu, dass Cross Site Request Forgeries (CSRF) fehlschlagen.

Eine sichere Verwaltungskonsolensitzung hat ein Leerlauf-Zeitlimit von fünf Minuten, und die Sitzung ist nur im aktuellen Browser-Fenster und/oder -Register gültig. Wenn der Benutzer versucht, die Sitzung in einem neuen Fenster oder Register zu öffnen, wird ein Sicherheitsfehler generiert, der eine gültige Sitzung anfordert. Durch diese Aktion wird auch verhindert, dass der Benutzer auf eine schädliche URL klickt, die die Verwaltungskonsolensitzung angreifen könnte.

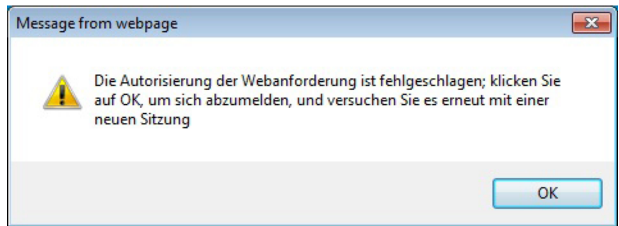


Abbildung 2. Fehlermeldung



Zugangskontrollauthentifizierung, -autorisierung und -rollen

OpenManage Integration for VMware vCenter verwendet die aktuelle Benutzersitzung des Web-Clients und speichert die Administratoranmeldeinformationen für OpenManage Integration zur Durchführung von vCenter-Vorgängen. OpenManage Integration for VMware vCenterverwendet die im vCenter-Server eingebauten Rollen- und Privilegien-Modelle, um Benutzervorgänge mit OpenManage Integration und verwalteten vCenter-Objekten (Hosts und Cluster) zu autorisieren. Greifen Sie auf die Rollen von der VMware vCenter-Startseite aus zu.



Dell-Vorgangsrolle

Enthält die Berechtigungen/Gruppen zur Ausführung von Geräte- und vCenter Server-Aufgaben einschließlich Firmware-Aktualisierungen, Hardware-Bestandslisten, Neustarten eines Hosts, Versetzen eines Hosts in den Wartungsmodus oder Erstellen einer vCenter Server-Aufgabe

Diese Rolle umfasst die folgenden Berechtigungsgruppen:

Berechtigungsgruppe – Dell.Konfiguration	Ausführen von, mit Hosts verknüpften, Aufgaben, Ausführen von, mit vCenter verknüpften, Aufgaben, Konfigurieren von SelLog, Konfigurieren von ConnectionProfile, Konfigurieren von ClearLed, Firmware-Aktualisierung
Berechtigungsgruppe – Dell.Bestandsaufnahme	Konfigurieren der Bestandsaufnahme, Konfigurieren des Garantieabrufs, Konfigurieren von ReadOnly
Berechtigungsgruppe – Dell.Überwachung	Konfigurieren der Überwachung, Überwachung
Berechtigungsgruppe – Dell.Berichterstellung (nicht verwendet)	Erstellen eines Berichts, Ausführen eines Berichts



Dell-Infrastrukturbereitstellungsrolle

Diese Rolle umfasst die Berechtigungen, die besonders mit den Hypervisor-Bereitstellungsfunktionen verknüpft sind.

Die von dieser Rolle gewährten Berechtigungen sind Erstellen von Vorlagen, Konfigurieren des HW-Konfigurationsprofils, Konfigurieren des Hypervisor-Bereitstellungsprofils, Konfigurieren des Verbindungsprofils, Zuweisen einer Identität und Bereitstellen.

Berechtigungsgruppe – Dell.Bereitstellung - Provisionierung	Erstellen von Vorlagen, Konfigurieren des HW-Konfigurationsprofils, Konfigurieren des Hypervisor-Bereitstellungsprofils, Konfigurieren des Verbindungsprofils, Zuweisen einer Identität, Bereitstellen



Grundlegende Informationen zu Berechtigungen

Jede vom OpenManage Integration for VMware vCenter ausgeführte Aktion ist einer Berechtigung zugeordnet. In den folgenden Abschnitten werden die verfügbaren Aktionen und die zugeordneten Berechtigungen aufgeführt:

- Dell.Konfiguration.Ausführen von mit vCenter verknüpften Aufgaben
  - Beenden und Starten des Wartungsmodus
  - Aufrufen der vCenter-Benutzergruppe zur Abfrage von Berechtigungen
  - Registrieren und Konfigurieren von Warnungen, z. B. Aktivieren/Deaktivieren von Warnungen auf der Seite mit den Ereigniseinstellungen
  - Veröffentlichen von Ereignissen/Warnungen bei vCenter
  - Konfigurieren von Ereigniseinstellungen auf der Seite mit den Ereigniseinstellungen
  - Wiederherstellen von Standardwarnungen auf der Seite mit den Ereigniseinstellungen
  - Überprüfen des DRS-Status auf Clustern während der Konfiguration von Warnungs-/Ereigniseinstellungen
  - Neustarten des Hosts nach Aktualisierungs- oder anderen Konfigurationsmaßnahmen
  - Überwachen des Status/Fortschritts von vCenter-Tasks
  - Erstellen von vCenter-Tasks, z. B. Firmware-Aktualisierungstask, Hostkonfigurationstask und Bestandsaufnahmetask
  - Aktualisieren des Status/Fortschritts von vCenter-Tasks
  - Abrufen von Hostprofilen
  - Hinzufügen von Hosts zu einem Datencenter
  - Hinzufügen von Hosts zu einem Cluster
  - Übernehmen des Profils für einen Host
  - Abrufen von CIM-Anmeldeinformationen
  - Konfigurieren von Hosts für Konformität
  - Abrufen des Status des Konformitätstasks
- Dell.Bestandsaufnahme.Konfigurieren von ReadOnly
  - Abrufen aller vCenter-Hosts zum Aufbau der vCenter-Struktur während der Konfiguration von Verbindungsprofilen
  - Bei Auswahl der Registerkarte überprüfen, ob der Host ein Dell-Server ist
  - Abrufen der Adresse/IP von vCenter
  - Abrufen der Host-IP/Adresse
  - Abrufen des Benutzers der aktuellen vCenter-Sitzung basierend auf der vSphere-Clientsitzungs-ID
  - Abrufen der vCenter-Bestandsaufnahmestruktur, um die vCenter-Bestandsliste in einer Baumstruktur anzuzeigen.
- Dell.Überwachung.Überwachen
  - Abrufen des Hostnamens für die Veröffentlichung des Ereignisses
  - Ausführen von Ereignisprotokollierungsvorgängen, z. B. Aufrufen der Ereignisanzahl oder Ändern der Ereignisprotokolleinstellungen
  - Registrieren, Aufheben der Registrierung und Konfigurieren von Ereignissen/Warnungen – Empfangen von SNMP-Traps und Veröffentlichen von Ereignissen

- Dell.Konfiguration.Firmware-Aktualisierung
  - Ausführen einer Firmware-Aktualisierung
  - Laden von Firmware-Repository- und DUP-Dateninformationen auf der Seite des Assistenten zur Firmware-Aktualisierung
  - Abfragen der Firmware-Bestandsliste
  - Konfigurieren der Firmware-Repository-Einstellungen
  - Konfigurieren des Stagingordners und Ausführen der Aktualisierung unter Verwendung der Stagingfunktion
  - Testen der Netzwerk- und Repository-Verbindungen
- Dell.Bereitstellung-Bereitstellen.Erstellen von Vorlagen
  - Erstellen, Anzeigen, Löschen und Bearbeiten der Bereitstellungsvorlagen
- Dell.Konfiguration.Ausführen von mit Hosts verknüpften Tasks
  - Blink-LED, Lösch-LED, Konfigurieren der OMSA-URL von der Registerkarte zur Dell-Serververwaltung
  - Starten der OMSA-Konsole
  - Starten der iDRAC-Konsole
  - Anzeigen und Löschen des SEL-Protokolls
- Dell.Bestandsaufnahme.Konfigurieren der Bestandsaufnahme
  - Anzeigen der Systembestandsliste auf der Registerkarte zur Dell-Serververwaltung
  - Abrufen von Speicherdetails
  - Abrufen von Stromüberwachungsdetails
  - Erstellen, Anzeigen, Bearbeiten, Löschen und Testen von Verbindungsprofilen auf der Seite mit den Verbindungsprofilen
  - Planen, Aktualisieren und Löschen des Bestandsaufnahmezeitplans
  - Ausführen einer Bestandsaufnahme auf Hosts

B

Grundlegendes zur automatischen Ermittlung

Die automatische Ermittlung ist ein Prozess, bei dem ein Dell PowerEdge-Bare-Metal-Server der 11., 12. oder 13. Generation zu einem Pool verfügbarer Server hinzugefügt wird, damit er von OpenManage Integration for VMware vCenter verwendet werden kann. Nachdem ein Server ermittelt wurde, können Sie ihn für die Hypervisor- und Hardware-Bereitstellung verwenden. In diesem Anhang finden Sie alle Informationen zur automatischen Ermittlung, die Sie für die Systemkonfiguration benötigen. Die automatische Ermittlung ist eine Lifecycle Controller-Funktion zum Einrichten und Registrieren eines neuen Servers mithilfe einer Konsole. Zu den Vorteilen dieser Funktion gehört zum einen, dass keine umständliche manuelle lokale Konfiguration des neuen Servers erforderlich ist, und zum anderen, dass ein neuer Server, nachdem er mit dem Netzwerk verbunden und an die Stromversorgung angeschlossen wurde, automatisch von der Konsole ermittelt wird.

Die automatische Ermittlung wird aufgrund der durchgeführten Prozesse auch als *Ermittlung und Handshake* bezeichnet. Wenn ein neuer Server mit aktivierter automatischer Ermittlung an die Stromversorgung angeschlossen und mit einem Netzwerk verbunden ist, versucht der Lifecycle Controller des Dell Servers, eine Bereitstellungskonsole zu *ermitteln*, die im Dell Bereitstellungsserver integriert ist. Die automatische Ermittlungsfunktion leitet dann einen sogenannten *Handshake* zwischen dem Bereitstellungsserver und dem Lifecycle Controller ein.

OpenManage Integration for VMware vCenter ist eine Bereitstellungskonsole mit integriertem Bereitstellungsserver. Der Speicherort des Bereitstellungsservers wird dem iDRAC auf unterschiedliche Weise mitgeteilt. Die IP-Adresse oder der Host-Name für den Speicherort des Bereitstellungsservers wird mit der IP-Adresse oder dem Host-Namen der virtuellen Maschine des OpenManage Integration for VMware vCenter-Geräts gleichgesetzt.



ANMERKUNG: Ein neuer Server, der für die automatische Ermittlung konfiguriert ist, versucht in einem Zeitraum von 24 Stunden alle 90 Sekunden, den Speicherort des Bereitstellungsservers aufzulösen. Nach diesem Zeitraum können Sie die automatische Ermittlung manuell erneut einleiten.

Beim Empfang der Anforderung für die automatische Ermittlung durch OpenManage Integration for VMware vCenter wird das SSL-Zertifikat validiert. Anschließend werden etwaige optional konfigurierte Sicherheitsverfahren eingeleitet, z. B. Abruf Client-seitiger Sicherheitszertifikate und Abgleich mit einer Whitelist. Anhand einer zweiten Validierungsanforderung seitens des neuen Servers werden die vorläufigen Anmeldeinformationen (Benutzername und Kennwort) ausgegeben, die auf dem iDRAC konfiguriert werden sollen. Anschließend werden von OpenManage Integration for VMware vCenter weitere Aufrufe initiiert. Dabei werden Informationen zum Server erfasst, die vorläufigen Anmeldeinformationen entfernt und dauerhafte benutzerdefinierte Anmeldeinformationen für den Verwaltungszugriff konfiguriert.

Wenn die automatische Ermittlung erfolgreich war, werden die zum Zeitpunkt der Ermittlung auf der Seite **Einstellungen** → **Bereitstellung** vorhandenen Anmeldeinformationen auf dem Ziel-iDRAC erstellt. Anschließend wird die automatische Ermittlung deaktiviert. Der Server müsste jetzt im Pool der verfügbaren Bare-Metal-Server unter „Bereitstellung" in OpenManage Integration for VMware vCenter angezeigt werden.

Die automatische Ermittlung kann zurzeit über den vSphere Desktop-Client erfolgen.

Voraussetzungen für die automatische Ermittlung

Bevor Sie versuchen Dell PowerEdge-Bare-Metal-Server der 11., 12. oder späteren Generation zu ermitteln, installieren Sie OpenManage Integration for VMware vCenter. Nur Dell PowerEdge-Server ab der 11. Generation mit iDRAC-Express oder iDRAC-Enterprise können im OpenManage Integration for VMware vCenter-Pool der Bare-Metal-Server ermittelt

werden. Es ist eine Netzwerkkonnektivität zwischen dem iDRAC des Dell Bare-Metal-Servers und der virtuellen Maschine des OpenManage Integration for VMware vCenter erforderlich.



ANMERKUNG: Hosts mit bereits vorhandenen Hypervisor sollten nicht durch das OpenManage Integration for VMware vCenter-Plugin ermittelt werden. Fügen Sie den Hypervisor stattdessen zu einem Verbindungsprofil hinzu und gleichen Sie ihn anschließend mithilfe des Assistenten für Host-Kompatibilität an das OpenManage Integration for VMware vCenter an.

Damit eine automatische Ermittlung stattfinden kann, müssen die folgenden Voraussetzungen erfüllt sein:

- **Strom:** Schließen Sie den Server an die Stromversorgung an. Der Server muss jedoch nicht eingeschaltet werden.
- **Netzwerkkonnektivität:** Der iDRAC des Servers muss über Netzwerkkonnektivität verfügen und über Port 4433 mit dem Bereitstellungsserver kommunizieren. Sie können die IP-Adresse über einen DHCP-Server anfordern oder diese manuell im iDRAC-Konfigurationshilfsprogramm angeben.
- **Zusätzliche Netzwerkeinstellungen:** Aktivieren Sie bei Verwendung von DHCP die Einstellung *DNS-Serveradresse über DHCP anfordern*, damit eine DNS-Namensauflösung erfolgen kann.
- **Speicherort des Bereitstellungsdienstes:** Dem iDRAC muss die IP-Adresse oder der Host-Name des Servers mit dem Bereitstellungsdienst bekannt sein.
- **Kontozugriff deaktiviert:** Aktivieren Sie den Zugriff des Verwaltungskontos auf den iDRAC. Falls iDRAC-Konten mit Administratorrechten vorhanden sind, müssen Sie diese zuerst über die iDRAC-Webkonsole deaktivieren. Nachdem die automatische Ermittlung erfolgreich durchgeführt wurde, wird das iDRAC-Verwaltungskonto wieder aktiviert.
- **Automatische Ermittlung aktiviert:** Auf dem iDRAC des Servers muss die Funktion für die automatische Ermittlung aktiviert sein, damit die automatische Ermittlung starten kann.

Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern

Damit Sie die automatische Ermittlung einrichten können, müssen Sie zuerst alle Verwaltungskonten, mit Ausnahme des Stammkontos, deaktivieren. Das Stammkonto wird im Rahmen der automatischen Ermittlung deaktiviert. Nachdem Sie die automatische Ermittlung erfolgreich eingerichtet haben, kehren Sie zurück zur GUI von Integrated Dell Remote Access Controller 6, und aktivieren Sie die Konten wieder, die Sie zuvor deaktiviert haben. Dieses Verfahren gilt für PowerEdge-Server der 11., 12. und 13. Generation.



ANMERKUNG: Als Schutzmaßnahme für den Fall des Fehlschlagens der automatischen Ermittlung können Sie ein Konto auf dem iDRAC aktivieren, das kein Verwaltungskonto ist. Auf diese Weise verfügen Sie über die Möglichkeit eines Remote-Zugriffs, falls die automatische Ermittlung fehlschlägt.

1. Geben Sie die **iDRAC-IP-Adresse** in einen Browser ein.
2. Melden Sie sich an der **GUI von Integrated Dell Remote Access Controller** an.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Bei iDRAC6: Wählen Sie im linken Fenster **iDRAC-Einstellungen** → **Netzwerk/Sicherheit** → **Benutzer** aus.
   - Bei iDRAC7: Wählen Sie im linken Fenster **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Benutzer** aus.
4. Machen Sie im Register „Benutzer“ alle Verwaltungskonten ausfindig, bei denen es sich nicht um das Stammkonto handelt.
5. Wählen Sie zum Deaktivieren eines Kontos unter „Benutzer-ID“ die entsprechende **ID** aus.
6. Klicken Sie auf **Weiter.**
7. Heben Sie auf der Seite „Benutzerkonfiguration“ unter „Allgemein“ die Markierung des Kontrollkästchens **Benutzer aktivieren** auf.
8. Klicken Sie auf **Anwenden**.

9. Nachdem Sie die automatische Ermittlung erfolgreich eingerichtet haben, müssen Sie die einzelnen Konten wieder aktivieren. Wiederholen Sie dazu die Schritte 1 bis 8, wobei Sie jedoch diesmal das Kontrollkästchen **Benutzer aktivieren** markieren und anschließend auf **Anwenden** klicken.

Manuelles Konfigurieren eines PowerEdge-Servers der 11. Generation für die automatische Ermittlung

Sie müssen über die iDRAC- und die Host-IP-Adresse verfügen.
Falls Sie Ihr Bare-Metal-Gerät nicht bereits mit werkseitiger Konfiguration für die automatische Ermittlung bestellt haben, können Sie die Funktion auch manuell einrichten. iDRAC verfügt über zwei Benutzerschnittstellen, die beide über die IP-Adresse des einzurichtenden iDRAC erreichbar sind.

Bei erfolgreicher automatischer Ermittlung der Bare-Metal-Server wird das neue Verwaltungskonto erstellt bzw. ein vorhandenes Konto mit den vom Handshake-Dienst übergebenen Anmeldeinformationen aktiviert. Alle anderen Verwaltungskonten, die vor der automatischen Ermittlung deaktiviert wurden, werden nicht automatisch wieder aktiviert. Sie müssen diese nach erfolgreichem Abschluss der automatischen Ermittlung selbst wieder aktivieren. Lesen Sie dazu den Abschnitt Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern.



ANMERKUNG: Falls die automatische Ermittlung aus irgendeinem Grund nicht vollständig durchgeführt wurde, gibt es primär keine Möglichkeit, eine Remote-Verbindung zum iDRAC herzustellen. Sie können eine solche Remote-Verbindung nur dann herstellen, wenn Sie auf dem iDRAC ein Konto aktiviert haben, das kein Verwaltungskonto ist. Falls auf dem iDRAC kein aktiviertes Konto vorhanden ist, können Sie nur auf den iDRAC zugreifen, indem Sie sich lokal am Gerät anmelden und das Konto auf dem iDRAC aktivieren.

1. Geben Sie die **iDRAC-IP**-Adresse in einen Browser ein.
2. Melden Sie sich an der **GUI von iDRAC Enterprise** an.
3. Klicken Sie im Register **Integrated Dell Remote Access Controller 6 – Enterprise** → **Systemzusammenfassung** in der Vorschau der virtuellen Konsole auf **Starten**.
4. Klicken Sie im Dialogfeld „Warnung – Sicherheit“ auf **Ja**.
5. Drücken Sie in der iDRAC-Programmkonsole einmal oder zweimal auf **F12**, um das Dialogfeld „Authentifizierung erforderlich“ aufzurufen.
6. Im Dialogfeld „Authentifizierung erforderlich“ wird der Name angezeigt. Drücken Sie die **Eingabetaste**.
7. Geben Sie Ihr **Kennwort** ein.
8. Drücken Sie die **Eingabetaste.**
9. Wenn das Dialogfeld „Herunterfahren/Neustart“ angezeigt wird, drücken Sie auf **F11**.
10. Der Host wird neu gestartet und der Bildschirm zeigt Informationen zum Laden des Speichers und dann zu RAID an. Wenn iDRAC angezeigt wird und Sie aufgefordert werden, die Tastenkombination STRG + E zu drücken, drücken Sie unverzüglich auf **STRG + E**.

    Wenn dieses Dialogfeld angezeigt wird, war Ihre Aktion erfolgreich. Wechseln Sie anderenfalls in das Menü „Strom“, schalten Sie das System aus und wieder ein, und wiederholen Sie den Vorgang.

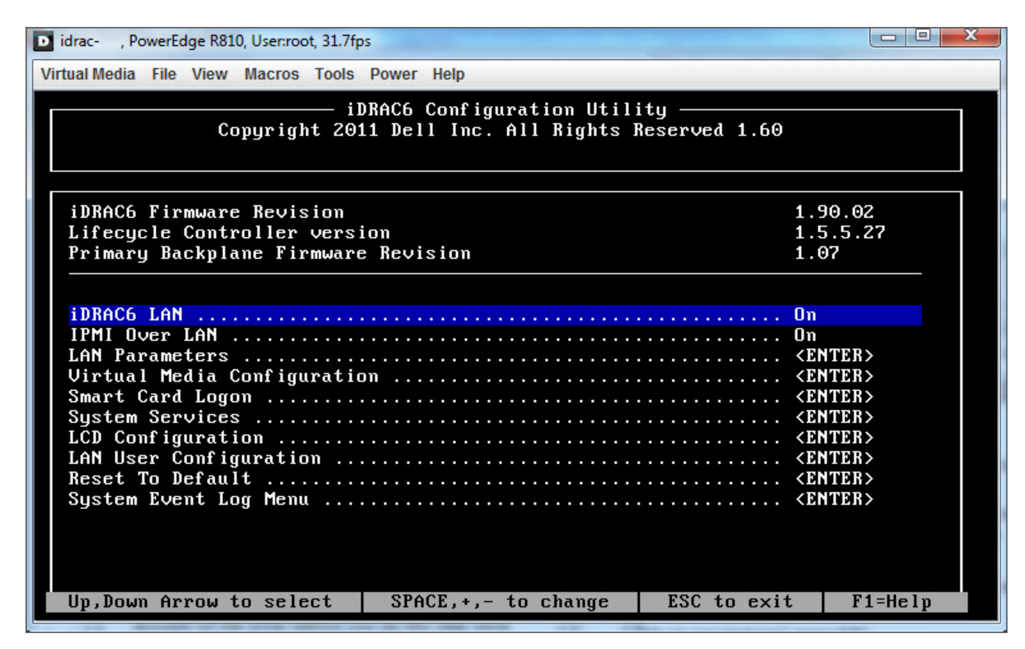


Abbildung 3. Drücken Sie die Tastenkombination STRG + E, um diesen Bildschirm zu aktivieren.

11. Markieren Sie im iDRAC6-Konfigurationshilfsprogramm mithilfe der Pfeiltasten die Option **LAN-Parameter**.
12. Drücken Sie die **Eingabetaste**.
13. Falls es sich bei diesem Host um ein Blade-System handelt, verwenden Sie zum Konfigurieren der NIC die Leertaste, um die Optionen auf **Aktiviert** zu setzen.
14. Wählen Sie bei Verwendung von DHCP mithilfe der Pfeiltasten die Option **Domänenname über DHCP** aus.
15. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
16. Wechseln Sie bei Verwendung von DHCP mithilfe der Pfeiltasten zu den IPv4-Einstellungen, und markieren Sie die Option **DNS-Server über DHCP**.
17. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
18. Drücken Sie zum Beenden die Taste **Esc** auf Ihrer Tastatur.
19. Markieren Sie mithilfe der Pfeiltasten die Option **LAN-Benutzerkonfiguration**.
20. Markieren Sie mithilfe der Pfeiltasten die Option **Bereitstellungsserver**.
21. Drücken Sie die **Eingabetaste**.
22. Geben Sie die IP-Adresse des Hosts ein.
23. Drücken Sie erneut auf **Esc**.
24. Markieren Sie mithilfe der Pfeiltasten die Option **Kontozugriff**.
25. Setzen Sie die Option mithilfe der Leertaste auf **Deaktivieren**.
26. Markieren Sie mithilfe der Pfeiltasten die Option **Automatische Ermittlung**.
27. Setzen Sie die Option mithilfe der Leertaste auf **Aktiviert**.
28. Drücken Sie auf Ihrer Tastatur auf **Esc**.
29. Drücken Sie ein zweites Mal auf **Esc**.

Manuelles Konfigurieren eines PowerEdge-Servers der 12. Generation und später für die Auto-Ermittlung

Sie müssen über die iDRAC- und die Host-IP-Adresse verfügen.

Falls Sie Ihr Bare-Metal-Gerät nicht bereits mit werkseitiger Konfiguration für die automatische Ermittlung bestellt haben, können Sie die Funktion auch manuell einrichten. iDRAC verfügt über zwei Benutzerschnittstellen, die beide über die IP-Adresse des einzurichtenden iDRAC erreichbar sind.

Bei erfolgreicher automatischer Ermittlung der Bare-Metal-Server wird das neue Verwaltungskonto erstellt bzw. ein vorhandenes Konto mit den vom Handshake-Dienst übergebenen Anmeldeinformationen aktiviert. Alle anderen Verwaltungskonten, die vor der automatischen Ermittlung deaktiviert wurden, werden nicht automatisch wieder aktiviert. Sie müssen diese nach erfolgreichem Abschluss der automatischen Ermittlung selbst wieder aktivieren. Lesen Sie dazu den Abschnitt Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern.



ANMERKUNG: Falls die automatische Ermittlung aus irgendeinem Grund nicht vollständig durchgeführt wurde, gibt es primär keine Möglichkeit, eine Remote-Verbindung zum iDRAC herzustellen. Sie können eine solche Remote-Verbindung nur dann herstellen, wenn Sie auf dem iDRAC ein Konto aktiviert haben, das kein Verwaltungskonto ist. Falls auf dem iDRAC kein aktiviertes Konto vorhanden ist, können Sie nur auf den iDRAC zugreifen, indem Sie sich lokal am Gerät anmelden und das Konto auf dem iDRAC aktivieren.

1. Geben Sie die **iDRAC-IP-Adresse** in einen Browser ein.
2. Melden Sie sich an der **GUI von iDRAC Enterprise** an.
3. Klicken Sie im Register **Integrated Dell Remote Access Controller 7 – Enterprise** → **Systemzusammenfassung** in der Vorschau der virtuellen Konsole auf **Starten**.
4. Klicken Sie im Dialogfeld „Warnung – Sicherheit“ auf **Ja**.
5. Drücken Sie in der iDRAC-Programmkonsole einmal oder zweimal auf **F12**, um das Dialogfeld „Authentifizierung erforderlich“ aufzurufen.
6. Im Dialogfeld „Authentifizierung erforderlich“ wird der Name angezeigt. Drücken Sie die **Eingabetaste**.
7. Geben Sie Ihr **Kennwort** ein.
8. Drücken Sie die **Eingabetaste.**
9. Wenn das Dialogfeld „Herunterfahren/Neustart“ angezeigt wird, drücken Sie auf **F11**.
10. Der Host wird neu gestartet und der Bildschirm zeigt Informationen zum Laden des Speichers und dann zu RAID an. Wenn ein Dell Bildschirm angezeigt wird, in dem Sie aufgefordert werden, die Taste F2 zu drücken, drücken Sie unverzüglich auf **F2**.

    Warten Sie, bis der Dell System-Setup-Bildschirm angezeigt wird. Dies kann einige Minuten dauern.
11. Markieren Sie im Dell System-Setup-Bildschirm mithilfe der Pfeiltasten die Option **iDRAC-Einstellungen**.
12. Markieren Sie mithilfe der Pfeiltasten die Option **Remote-Aktivierung**.
13. Klicken Sie zum Aktivieren der automatischen Ermittlung auf **Aktivieren**.
14. Drücken Sie auf **Esc**.
15. Drücken Sie erneut auf **Esc**.
16. Klicken Sie im Warnungsbildschirm auf **Ja**, um den Vorgang des Beendens zu bestätigen.